Alcatel·Lucent

Alcatel-Lucent 1665

Data Multiplexer (DMX) | Release 9.1

Alarm Messages and Trouble Clearing Guide

365-372-302R9.1
Issue 1
November 2011

Legal notice

Conformance statements

Federal Communications Commission (FCC) Part 15 Class A

This equipment has been tested and found 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 protections 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 instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user’s expense.

Security statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of remote access features. In such an event, applicable tariffs require that the customer pay all network charges for traffic. Alcatel-Lucent cannot be responsible for such charges and will not make any allowance or give any credit for charges that result from unauthorized access.

Limited warranty

Alcatel-Lucent provides a limited warranty for this product. For more information, consult your local Alcatel-Lucent customer support team.

Contents

List of tables

List of figures

List of procedures

5 Trouble-clearing procedures

About this document

Purpose

This *Alarm Messages and Trouble Clearing Guide* provides the following information about the Alcatel-Lucent 1665 Data Multiplexer (Alcatel-Lucent 1665 DMX), Release 9.1:

- Maintenance and trouble-clearing information and procedures
- A central directory of alarm messages

Reason for reissue

This document is issued to provide information about Release 9.1 features, including:

- In-service upgrades
  - LNW82 to LNW59 one port upgrade
  - LNW59 to LNW504 one or two port upgrade
  - LNW56, LNW57, LNW58, and LNW502 to LNW504 upgrade
- LNW7 to LNW801 DS1 capacity upgrade
- LNW8 and LNW801 can exist in the same function group
- Change the initial default state of an external timing reference from Auto to IS
- STS-192c cross-connect support
- Bi-directional ALS on LNW63/64/70/74/87/170
- FEC is provisionable on LNW705
- Additional buffer sizes for FE and GigE for LNW63/70/74/170
- In TL1 cut-through, the last TID specified is remembered and used in all subsequent commands in which a TID is not specified.
- Extra traffic on low-speed or high-speed OC-192 BLSRs when the mains are equipped with VLF packs
- Optional OOS check for loopback on Ethernet, PDH and EC-1 signals
- Ethernet loopbacks are allowed even when RCF or FEFI are active
- Microsoft *Windows*® 7 64-bit, support on *WaveStar*® CIT

Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

Intended audience

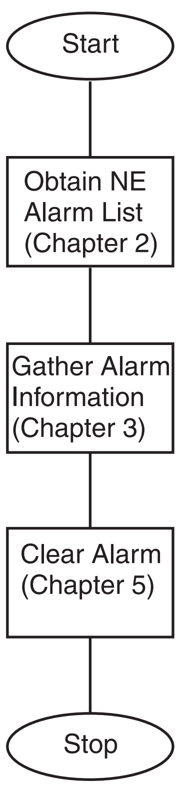
This *Alarm Messages and Trouble Clearing Guide* is intended primarily for telecommunications technicians and communications network providers.

Procedural information in this document is intended primarily for maintenance, operation, and provisioning personnel responsible for operating and maintaining the Alcatel-Lucent 1665 Data Multiplexer.

How to use this information product

This guide includes descriptive and procedure chapters with supporting information (for example, safety instructions, glossary, and index). Refer to the Contents section to locate specific information.

Refer to the following flow chart when clearing network element alarms and conditions.



flowchart-1

Assumptions

This document assumes that users have an understanding of the following:

- Basic principles of telecommunication transmission
- Common telecommunication and system terminology (a glossary is provided in this document to assist you)
- Test sets and tools used in the telecommunication industry
- Local operations and functional procedures of your company
- Personal computer (PC) operation, common PC terminology, and navigational procedures in a windows-style user interface

Conventions used

The following conventions are used in this document.

- **`This font`** indicates a command.

  Example:

  `ent-user-secu`
- *This font* indicates a document reference.

  Example:

  Alcatel-Lucent 1665 Data Multiplexer (DMX) Applications and Planning Guide, 365-372-300 (document title and 9-digit ordering number)
- **This font** indicates buttons, icons, or menu items.

  Example:

  Configuration → **Equipment**
- *This font* indicates window names or special emphasis.

  Example:

  The *Configure Equipment* window is displayed.
- **This font** indicates lettering designations on the backplane, shelf, and circuit packs.

  Example:

  Release the **ACO TEST** push button on the SYSCTL circuit pack faceplate when the **8.** disappears in the **IND** display.
- `This font` indicates information that is either output by the system or is displayed on the computer.

  Example:

  The response will be `/* SYSTEM TID: LT-DMX */`.
- Blue text indicates hyperlinks (cross-references) to other text in the document or another step in the procedure.

  Example: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)
- Important messages are displayed as follows:

  Important! This is important information.

User interface to system

You will interact with the Alcatel-Lucent 1665 Data Multiplexer using a PC and a windows-based graphical user interface (GUI). The GUI is called the *WaveStar®* Craft Interface Terminal (*WaveStar®* CIT) and permits system operations to be performed (for example, administration, provisioning, and fault management).

Using the *WaveStar®* CIT

Procedures presented in this document expect you to be familiar with the *WaveStar®* CIT and with navigation windows. The windows are designed to be straightforward and to contain all information relating to a particular operation. The procedures presented in this document rely on the information provided in the window displays. Therefore, it is imperative that you read all the information provided in a window before continuing an operational function.

Using procedures

To find instructions for performing a specific job, first determine the procedure category (for example, trouble-clearing). After determining the procedure category, go to the corresponding procedure chapter and find the procedure in the chapter *Contents* table.

The procedures in Chapter 5, “Trouble-clearing procedures”, contain step-by-step instructions to accomplish a distinct user job.

The procedures in Chapter 6, “Supporting procedures”, are referenced from multiple procedures to support a job function you are performing. Proceed to a supporting procedure only when it is referred to by another procedure. Supporting procedures are not to be accessed directly except by very experienced personnel.

> **Important!** Perform all steps in a procedure sequentially, unless that step sends you to another step or procedure.
>
> Unless otherwise instructed, if one procedure sends you to another procedure, you must return to the first procedure after you complete the second. After you have completed the first procedure element, you have finished.

If/Then statements in a procedure

If …/Then … columns in a procedure contain only one condition that is true in a table cell under the If … column. Perform the action in the related table cell under the Then … column. Then continue to the next sequential step or as directed by the action under the Then … column.

Verifying actions

Sometimes you will be asked to verify that actions have occurred. This may take the form of a formal statement with the expected response. At other times, you will be instructed to merely verify that the action occurred. If the expected response is not observed and a specific trouble-clearing reference is not made, reference the *Trouble-clearing procedures* chapter in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Alarm Messages and Trouble Clearing Guide, 365-372-302*, to start trouble-clearing.

Related information

The following table lists the documents included in the Alcatel-Lucent 1665 DMX documentation set.

Table 1 Alcatel-Lucent 1665 DMX documentation set

Document number/Comcode	Title
365-372-330	*WaveStar® User Guide*
365-372-300R9.1	*Alcatel-Lucent 1665 Data Multiplexer (DMX) Applications and Planning Guide*
365-372-301R9.1	*Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide*
365-372-302R9.1	*Alcatel-Lucent 1665 Data Multiplexer (DMX) Alarm Messages and Trouble Clearing Guide*
365-372-304R9.1	*Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual*
365-372-306R9.1	*Alcatel-Lucent 1665 Data Multiplexer (DMX) TL1 Message Details*
ED8C871-10	*Alcatel-Lucent 1665 Data Multiplexer (DMX) Engineering and Ordering Information*
ED8C871-20	*Alcatel-Lucent 1665 Data Multiplexer (DMX) Interconnect Information*
109783647	*Alcatel-Lucent 1665 Data Multiplexer (DMX) Release 9.1.0 Customer Release Notes* (PDF)
109783274	*Alcatel-Lucent 1665 Data Multiplexer (DMX) Release 9.1.0 Customer Release Notes* (CD-ROM)
109783282	*Alcatel-Lucent 1665 Data Multiplexer (DMX) Release 9.1.X Customer Documentation CD-ROM*

Technical support

For technical support, contact your local Alcatel-Lucent customer support team. See the Alcatel-Lucent Support web site (http://alcatel-lucent.com/support/) for contact information.

How to order

To order Alcatel-Lucent documents, contact your local sales representative or use Online Customer Support (OLCS) (http://support.alcatel-lucent.com).

How to comment

To comment on this document, go to the Online Comment Form (http://infodoc.alcatel-lucent.com/comments/) or e-mail your comments to the Comments Hotline (comments@alcatel-lucent.com).

1 Safety

Overview

Purpose

This chapter provides important safety instructions for Alcatel-Lucent 1665 DMX.

Contents

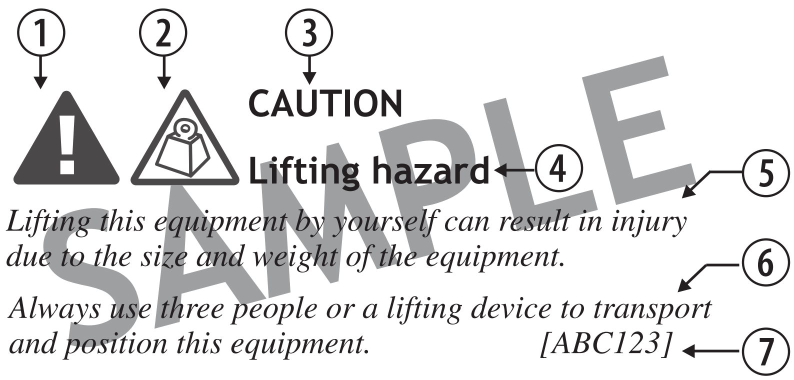
Structure of safety statements

Overview

This topic describes the components of safety statements that appear in this document.

General structure

Safety statements include the following structural elements:



Item	Structure element	Purpose
1	Safety alert symbol	Indicates the potential for personal injury (optional)
2	Safety symbol	Indicates hazard type (optional)
3	Signal word	Indicates the severity of the hazard
4	Hazard type	Describes the source of the risk of damage or injury
5	Safety message	Consequences if protective measures fail
6	Avoidance message	Protective measures to take to avoid the hazard
7	Identifier	The reference ID of the safety statement (optional)

Signal words

The signal words identify the hazard severity levels as follows:

Signal word	Meaning
DANGER	Indicates an extremely hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a hazardous situation not related to personal injury.

General notes on safety

Overview

All responsible technical personnel *must* read this chapter before servicing the system. Always keep the most recent issue of this document close to the equipment.

In addition to the general safety instructions in this chapter, users must also observe the specific safety instructions in the individual chapters.

The equipment complies with the current national and international safety requirements. It is provided with a high degree of operational safety resulting from many years of development experience and continuous stringent quality checks.

Potential sources of danger

The equipment is safe in normal operation. However, some potential sources of danger cannot be completely eliminated. In particular, these may arise during the following operations:

- Opening of housings or equipment covers
- Manipulation of any kind within the equipment, even if it has been disconnected from the power supply
- Disconnection of optical or electrical connections
- Through possible contact with live pairs, laser light, hot surfaces, sharp edges, or components sensitive to electrostatic discharge

Special safety instructions

Laser safety and *handling components sensitive to electrostatic discharge (ESD)* are vitally important to the equipment. For special safety instructions concerning laser safety and electrostatic discharge, refer to sections "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26).

General safety requirements

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

- Transport, storage, and operation of the unit/system must be under the *permissible conditions only*.

  See accompanying documentation and information on the unit/system.
- Installation, configuration, and disassembly must be performed only by *expert personnel* referring to *the respective documentation*.

  Due to the complexity of the unit/system, the personnel performing installation, configuration, and disassembly require *special training*.
- *Expert* and *authorized users* are required to operate the unit/system.

Operate the unit/system only after having *read and understood* the chapter on safety and the parts of the documentation relevant to operation. For complex systems, additional training is recommended. Any obligatory training for operating and service personnel must be carried out and documented.

- Do not operate the unit/system unless it is in perfect working order.

  Immediately report any faults or errors that might affect safety.
- Operate the unit/system with the proper connections and under the environmental conditions as described in the documentation.
- Only qualified Alcatel-Lucent personnel or expert personnel authorized by Alcatel-Lucent are permitted to perform conversions or changes to the system or parts of the system (including the software).

  All changes performed by other persons lead to a *complete exemption from liability*.

  Do not use components or spare parts that are not recommended by the manufacturer and those not listed in the procurement documents.
- Only *specially qualified personnel* are permitted to remove or disable safety facilities, clear faults and errors, and maintain the equipment.

  Strictly observe the respective parts of the documentation, and consult the documentation during the selection of measurement and test equipment.
- Document and archive all work related to calibrations, special tests after repairs, and regular safety checks.
- Use non-system software at your *own risk*. The use/installation of non-system software can adversely affect the normal functioning of the unit/system.

Laser safety

System compliance

Alcatel-Lucent 1665 DMX complies with the following laser safety regulations and standards:

- Alcatel-Lucent declares that Alcatel-Lucent 1665 DMX contains as Class 1M laser products are certified under the International Electrotechnical Commission (IEC) standards IEC 60825-1 Edition 1.0 and its amendment 1 (1997) and amendment 2 (2001) and IEC 60825-2 Edition 3.1 (2007). It is a Class I/1 laser optical fiber communication systems "product" under the IEC classification.
- Alcatel-Lucent declares that Alcatel-Lucent 1665 DMX contains as Class 1M laser products that are certified under the CENELEC standards EN 60825-1 Edition 1994 and its amendment 1 (2002) and amendment 2 (2001) and IN 60825-2 Edition 2004.
- Alcatel-Lucent declares that Alcatel-Lucent 1665 DMX contains as Class IIIb laser products that are certified under the regulations 21 CFR 1040.10 and 1040.11, which are implemented by the Food and Drug Administration's Center for Devices and Radiological Health (FDA/CDRH).

This Product is designed to ensure that personnel operating the product are not endangered by laser radiation during normal operation and fault conditions. This product does not present a risk of eye injury because it is fully enclosed and does not contain embedded lasers greater than Class I/1 unless otherwise noted.

The following table shows the optical circuit pack laser safety specifications. The pluggable transmission modules (and the supported circuit packs) are covered in Table 1-2, "Pluggable transmission module laser safety specifications" (p. 1-8).

Table 1-1 Optical circuit pack laser safety specifications

Laser Circuit Pack Code	Wavelength (nm)	Output Power (dBm)	Fiber Type (µm)	Connector Type	FDA Class/ IEC Class
LNW36 OC-3[1]	1310	0.0	Single Mode (9)	LC	I(LN50)/1
LNW46 OC-12[1]	1310	+2.0	Single Mode (9)	LC	I(LN50)/1
LNW48 OC-12	1310	−8.0	Single Mode (9)	LC	I(LN50)/1
LNW50 OC-12	1310	+2.0	Single Mode (9)	LC	I(LN50)/1
LNW54 OC-12	1550	+2.0	Single Mode (9)	LC	I(LN50)/1
LNW26B OC-48[1]	1310	+3.0	Single Mode (9)	LC	I(LN50)/1
LNW27 OC-48	1310	+3.0	Single Mode (9)	LC	I(LN50)/1
LNW28 OC-48[1]	1310	+3.0	Single Mode (9)	LC	I(LN50)/1
LNW29 OC-48	1550	+3.0	Single Mode (9)	LC	I(LN50)/1

Table 1-1 Optical circuit pack laser safety specifications (continued)

Laser Circuit Pack Code	Wavelength (nm)	Output Power (dBm)	Fiber Type (µm)	Connector Type	FDA Class/ IEC Class
LNW31 OC-48	1310	0.0	Single Mode (9)	LC	I(LN50)/1
LNW32 OC-48	1310	+3.0	Single Mode (9)	LC	I(LN50)/1
LNW76 OC-48	1310	−3.0	Single Mode (9)	LC	I(LN50)/1
LNW77 OC-48[1]	1310	0.0	Single Mode (9)	LC	I(LN50)/1
LNW121B–159B OC-48[1]	1550–range	+2.0	Single Mode (9)	LC	I(LN50)/1
LNW221–259 OC-48[1]	1550–range	+2.0	Single Mode (9)	LC	I(LN50)/1
LNW421–459 OC-48[1]	1550–range	+2.0	Single Mode (9)	LC	I(LN50)/1
LNW56 OC-192	1550	+2.0	Single Mode (9)	LC	I(LN50)/1
LNW57 OC-192[1]	1550	+6.0	Single Mode (9)	LC	I(LN50)/1
LNW58 OC-192	1310	−1.0	Single Mode (9)	LC	I(LN50)/1
LNW60 OC-192[1]	1550	+12.5	Single Mode (9)	LC	IIIb/1M
LNW523 OC-192[1]	1550–range	+6.0	Single Mode (9)	LC	I(LN50)/1
LNW527 OC-192[1]	1550–range	+6.0	Single Mode (9)	LC	I(LN50)/1
LNW554 OC-192[1]	1550–range	+6.0	Single Mode (9)	LC	I(LN50)/1
LNW555 OC-192[1]	1533.465	+6.0	Single Mode (9)	LC	I(LN50)/1

Notes:

1. DA'ed and no longer available.

The following table shows the pluggable transmission module (PTM) laser safety specifications and the supported circuit packs. Use only the following Alcatel-Lucent approved Class 1 SFP/XFP transceivers.

Table 1-2 Pluggable transmission module laser safety specifications

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (µm)	Connector Type	FDA Class/ IEC Class
100BASE-FX-I1	LNW70 LNW74 LNW78 LNW87 LNW170	1310	−14.0	Multimode (50 and 62.5)	LC	I(LN50)/1
100BASE-LX-I1	LNW70 LNW74 LNW78 LNW87 LNW170	1310	−8.0	Single Mode (9)	LC	I(LN50)/1
100BASE-ZX-I1	LNW87 LNW170	1550	+2.0	Single Mode (9)	LC	I(LN50)/1
1000BASE-ZX-I1	LNW63 LNW64 LNW70 LNW78 LNW87 LNW170	1550	+5.0	Single Mode (9)	LC	I(LN50)/1
BASE-T-C1 electrical	LNW63 LNW64 LNW70 LNW78 LNW87 LNW170	NA	NA	NA	RJ45	NA
ESCON-MM-I1	LNW73/73C	1310	−14.0	Multimode (50 and 62.5)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (μm)	Connector Type	FDA Class/ IEC Class
GE-1X2XFC-LX-I1	LNW63 LNW64 LNW70 LNW73/73C LNW78 LNW87 LNW170 LNW705	1310	−3.0	Single Mode (9)	LC	I(LN50)/1
GE-1X2XFC-SX-I1	LNW63 LNW64 LNW70 LNW73/73C LNW78 LNW87 LNW170 LNW705	850	−2.5	Multimode (50 and 62.5)	LC	I(LN50)/1
OC3IR1-I1	LNW37 LNW45 LNW55 LNW82 LNW705	1310	−8.0	Single Mode (9)	LC	I(LN50)/1
OC3LR1-I1	LNW37 LNW45 LNW55 LNW82 LNW705	1310	0.0	Single Mode (9)	LC	I(LN50)/1
OC-3SR1 (S155I2)	LNW37 LNW45 LNW55 LNW82 LNW705	1310	−8.0	Single Mode (9)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (μm)	Connector Type	FDA Class/ IEC Class
OC3X12X48-IR1-I1	LNW55 LNW82	1310	0.0	Single Mode (9)	LC	I(LN50)/1
OC3X12X48-LR1-I1	LNW55 LNW82	1310	3.0	Single Mode (9)	LC	I(LN50)/1
OC12IR1-I1	LNW49 LNW55 LNW82 LNW203 LNW705	1310	−8.0	Single Mode (9)	LC	I(LN50)/1
OC12LR1-I1	LNW49 LNW55 LNW82 LNW203 LNW705	1310	+2.0	Single Mode (9)	LC	I(LN50)/1
OC12LR2-I1	LNW49 LNW55 LNW82 LNW203 LNW705	1550	+2.0	Single Mode (9)	LC	I(LN50)/1
OC48LR1-I1	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504 LNW705	1310	+3.0	Single Mode (9)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (µm)	Connector Type	FDA Class/ IEC Class
OC48LR2-I1	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504 LNW705	1550	+3.0	Single Mode (9)	LC	I(LN50)/1
OC48SR1-I1	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504 LNW705	1310	−3.0	Single Mode (9)	LC	I(LN50)/1
OC192IR2-C1	LNW59 LNW502 LNW504 LNW603 LNW705	1550	+2.0	Single Mode (9)	LC	I(LN50)/1
OC192IR2-I1	LNW59 LNW705	1550	+2.0	Single Mode (9)	LC	I(LN50)/1
OC192LR2- C1	LNW59 LNW502 LNW504 LNW603 LNW705	1550	+4.0	Single Mode (9)	LC	I(LN50)/1
OC192SR1- C1	LNW59 LNW502 LNW504 LNW603 LNW705	1310	−1.0	Single Mode (9)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (µm)	Connector Type	FDA Class/ IEC Class
S2D23C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1558.983	+4.0	Single Mode (9)	LC	I(LN50)/1
S2D25C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1557.363	+4.0	Single Mode (9)	LC	I(LN50)/1
S2D27C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1555.747	+4.0	Single Mode (9)	LC	I(LN50)/1
S2D31C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1552.524	+4.0	Single Mode (9)	LC	I(LN50)/1
S2D33C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1550.918	+4.0	Single Mode (9)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (µm)	Connector Type	FDA Class/ IEC Class
S2D35C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1549.315	+4.0	Single Mode (9)	LC	I(LN50)/1
S2D37C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1547.715	+4.0	Single Mode (9)	LC	I(LN50)/1
S2D45C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1541.349	+4.0	Single Mode (9)	LC	I(LN50)/1
S2D47C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1539.766	+4.0	Single Mode (9)	LC	I(LN50)/1
S2D49C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1538.186	+4.0	Single Mode (9)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (μm)	Connector Type	FDA Class/ IEC Class
S2D53C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1535.036	+4.0	Single Mode (9)	LC	I(LN50)/1
S2D55C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1533.465	+4.0	Single Mode (9)	LC	I(LN50)/1
S2D59C6 (OC-48/STM–16/ OTU1 DWDM)	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504	1530.334	+4.0	Single Mode (9)	LC	I(LN50)/1
S2G7C47LI (OC48/STM16 CWDM)	VLNC55 VLNC62 LNW82 LNW202 LNW402 LNW504	1471	+5.0	Single Mode (9)	LC	I(LN50)/1
S2G7C49LI (OC48/STM16 CWDM)	VLNC55 VLNC62 LNW82 LNW202 LNW402 LNW504	1491	+5.0	Single Mode (9)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (μm)	Connector Type	FDA Class/ IEC Class
S2G7C51LI (OC48/STM16 CWDM)	VLNC55 VLNC62 LNW82 LNW202 LNW402 LNW504	1511	+5.0	Single Mode (9)	LC	I(LN50)/1
S2G7C53LI (OC48/STM16 CWDM)	VLNC55 VLNC62 LNW82 LNW202 LNW402 LNW504	1531	+5.0	Single Mode (9)	LC	I(LN50)/1
S2G7C55LI (OC48/STM16 CWDM)	VLNC55 VLNC62 LNW82 LNW202 LNW402 LNW504	1551	+5.0	Single Mode (9)	LC	I(LN50)/1
S2G7C57LI (OC48/STM16 CWDM)	VLNC55 VLNC62 LNW82 LNW202 LNW402 LNW504	1571	+5.0	Single Mode (9)	LC	I(LN50)/1
S2G7C59LI (OC48/STM16 CWDM)	VLNC55 VLNC62 LNW82 LNW202 LNW402 LNW504	1591	+5.0	Single Mode (9)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (µm)	Connector Type	FDA Class/ IEC Class
S2G7C61LI (OC48/STM16 CWDM)	LNW82 LNW202 LNW402 LNW504	1611	+5.0	Single Mode (9)	LC	I(LN50)/1
S622C47EL (OC-3/STM-1/OC-12/STM-4 CWDM)	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705	1471	+5.0	Single Mode (9)	LC	I(LN50)/1
S622C49EL (OC-3/STM-1/OC-12/STM-4 CWDM)	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705	1491	+5.0	Single Mode (9)	LC	I(LN50)/1
S622C51EL (OC-3/STM-1/OC-12/STM-4 CWDM)	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705	1511	+5.0	Single Mode (9)	LC	I(LN50)/1
S622C53EL (OC-3/STM-1/OC-12/STM-4 CWDM)	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705	1531	+5.0	Single Mode (9)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (µm)	Connector Type	FDA Class/ IEC Class
S622C55EL (OC-3/STM-1/OC-12/STM-4 CWDM)	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705	1551	+5.0	Single Mode (9)	LC	I(LN50)/1
S622C57EL (OC-3/STM-1/OC-12/STM-4 CWDM)	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705	1571	+5.0	Single Mode (9)	LC	I(LN50)/1
S622C59EL (OC-3/STM-1/OC-12/STM-4 CWDM)	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705	1591	+5.0	Single Mode (9)	LC	I(LN50)/1
S622C61EL (OC-3/STM-1/OC-12/STM-4 CWDM)	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705	1611	+5.0	Single Mode (9)	LC	I(LN50)/1
X10G21C5 (OC-192/STM-64/OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1560.606	+3.0	Single Mode (9)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (μm)	Connector Type	FDA Class/ IEC Class
X10G22C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1559.794	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G23C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1558.983	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G24C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1558.173	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G25C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1557.363	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G26C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1556.555	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G27C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1555.747	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G28C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1554.940	+3.0	Single Mode (9)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (µm)	Connector Type	FDA Class/ IEC Class
X10G31C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW504 LNW603 LNW705	1552.524	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G33C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW504 LNW603 LNW705	1550.918	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G35C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW504 LNW603 LNW705	1549.315	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G37C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW504 LNW603 LNW705	1547.715	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G45C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW504 LNW603 LNW705	1541.349	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G47C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW504 LNW603 LNW705	1539.766	+3.0	Single Mode (9)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (µm)	Connector Type	FDA Class/ IEC Class
X10G49C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW504 LNW603 LNW705	1538.186	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G52C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1535.822	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G53C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1535.036	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G54C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1534.250	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G55C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1533.465	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G56C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1532.681	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G57C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1531.898	+3.0	Single Mode (9)	LC	I(LN50)/1

Table 1-2 Pluggable transmission module laser safety specifications (continued)

Module Code	Supported Circuit Packs	Wavelength (nm)	Output Power (dBm)	Fiber Type (µm)	Connector Type	FDA Class/ IEC Class
X10G58C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1531.116	+3.0	Single Mode (9)	LC	I(LN50)/1
X10G59C5 (OC-192/STM-64/ OTU2 DWDM)	LNW59 LNW502 LNW603 LNW705	1530.334	+3.0	Single Mode (9)	LC	I(LN50)/1

Notes:

1. DA'ed and no longer available.

General laser information

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

Conventional lasers can produce an intense beam of monochromatic light. Monochromatic light is a single wavelength output of pure color that may be visible or invisible to the eye. A conventional laser produces a small-sized 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 four) and rapidly decreases over distance.

Lasers and eye damage

The optical energy emitted by laser and high-radiance LEDs in the 400 to 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 higher than at the cornea and, if sufficiently intense, may cause a retinal burn.

The damage mechanism at the wavelengths used in optical fiber telecommunications is thermal in origin; for example, 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 corneal and skin burns, but these optical energies 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 the following classes: I, II, lla, IIIa, lllb, or IV.

The International Electrotechnical Commission (IEC) is an international standards body that writes laser safety standards under IEC-60825. Classification schemes are similar and divided into Classes 1, 1M, 2, 2M, 3B, 3R, and 4. Lasers are classified according to the accessible emission limits and their potential for causing injury.

Optical fiber telecommunication systems are generally classified as Class I/1, because, under normal operating conditions, all energized laser transmitting circuit packs are terminated on optical fibers which enclose the laser energy with the fiber sheath forming a protective housing. Also, a protective housing/access panel is typically installed in front of the laser circuit pack shelves. The circuit packs themselves, however, may be FDA/CDRH Class I, IIIb, or IV or IEC Class 1, 1M, 3B, 3R, or 4. State-of-the-art Raman and EDFA optical amplifiers have now extended into the Class IV/4 designations.

Laser safety precautions for optical fiber telecommunications systems

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

The fiber optic cables that interconnect various components of an optical fiber telecommunication system can disconnect or break and may expose people to lightwave emission. Also, certain measurements 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. If you inadvertently view an unterminated fiber or damaged fiber with the unaided eye at distances greater than 5 to 6 inches, normally, it will not cause eye injury provided that the power in the fiber is less than a few milliwatts at the near IR wavelengths and a few tens of milliwatts at the far IR wavelengths. However, damage may occur if you use an optical instrument such as a microscope, magnifying glass, or eye loupe to stare at the energized fiber end.

Laser radiation

WARNING

Laser hazard

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

Do not view directly into the laser beam with optical instruments such as a fiber microscope because viewing of laser emission in excess of Class 1 limits significantly increases the risk of eye damage.

Never look into the end of an exposed fiber or an open connector as long as the optical source is switched on.

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

Laser safety precautions for enclosed systems

Under normal operating conditions, optical fiber telecommunication systems are completely enclosed. Observe the following laser safety precautions for enclosed systems:

- Because of the potential for eye damage, do not stare into optical connectors or broken fibers.
- Do not under any circumstances perform laser/fiber optic operations before satisfactorily completing laser safety training.
- 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, observe/follow laser safety labels. Appropriate labels must appear in plain view, in close proximity to the optical port on the protective housing/access panel of the terminal equipment

Laser safety precautions for unenclosed systems

During service, maintenance, or restoration, an optical fiber telecommunication system is considered unenclosed. Observe the following laser safety precautions for unenclosed systems:

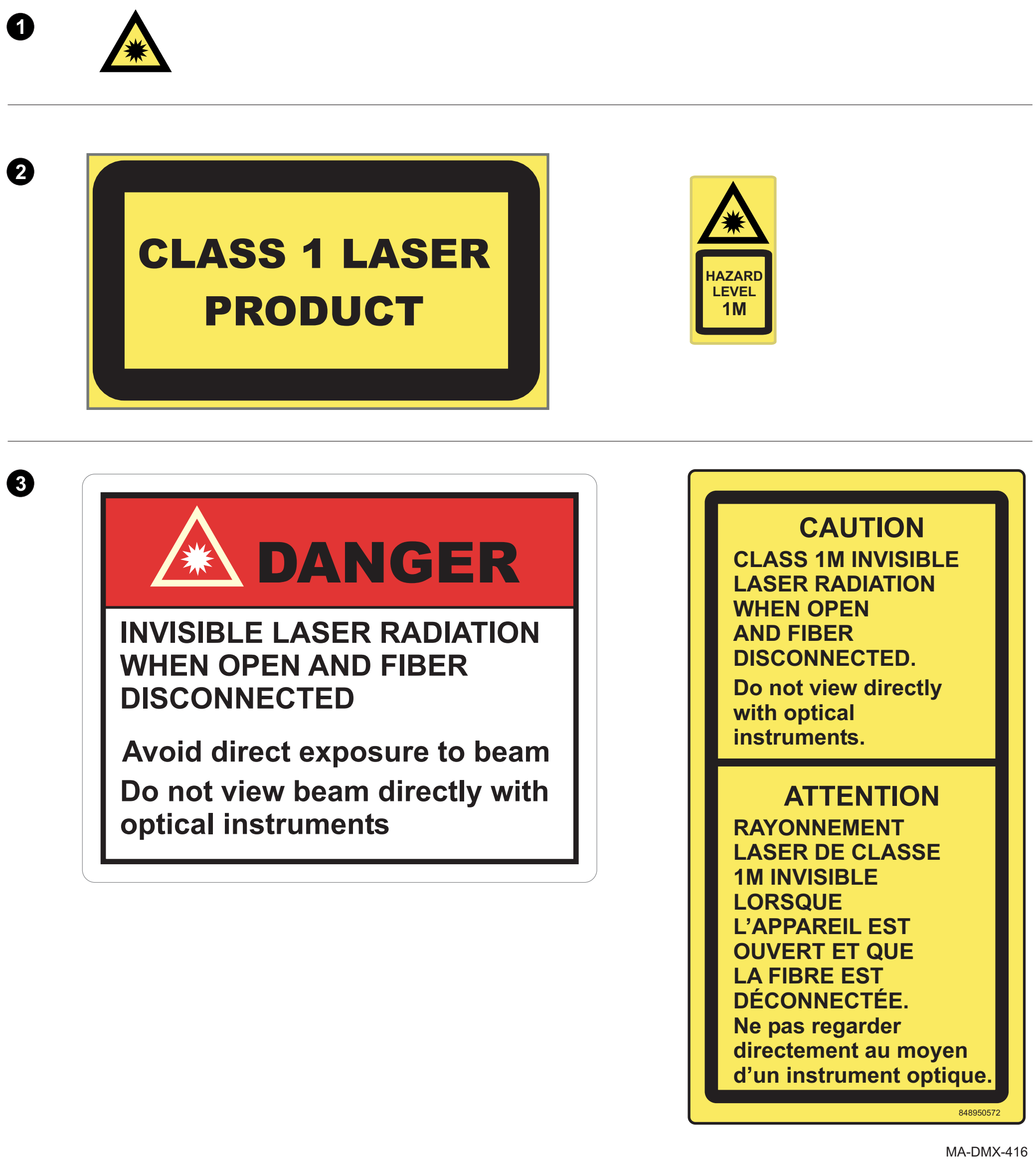
- Only authorized, trained personnel shall be permitted to do service, maintenance, and restoration. Avoid exposing the eye to emissions from unterminated, energized optical connectors at close distances. Laser modules associated with the optical ports of laser circuit packs are typically recessed, which limits the exposure distance. Optical port shutters, automatic power reduction (APR), and automatic power shutdown (APSD) are engineering controls that are also used to limit the emissions. However, do not stare or look directly into the optical port with optical instruments or magnifying lenses when removing or replacing laser circuit packs. (Normal eye wear or indirect viewing instruments, such as a Find-R-Scopes, are not considered magnifying lenses or optical instruments.)
- Only authorized, trained personnel shall use the optical test equipment during installation or servicing since this equipment contains semiconductor lasers. (Some examples of optical test equipment are Optical Time Domain Reflectometers [OTDRs] and Hand-Held Loss Test Sets.)
- Do not, under any circumstance, scan a fiber with an optical test set without verifying that all laser sources on the fiber are turned off.
- Only authorized personnel are permitted in the immediate area of the optical fiber telecommunication systems during installation and service.

For guidance on the safe use of optical fiber optic communication systems in the workplace, consult *ANSI* Z136.2, American National Standard for Safe Use of Optical Fiber Communication Systems Utilizing Laser Diodes and LED Sources in the United States or outside the United States, IEC-60825, Part 2.

Laser warning labels

The following figure shows the different types of laser warning labels:

Figure 1-1 Laser warning labels



Legend

1. Laser symbol

2. Laser classification labels (This label may show only the laser class or both the laser class and the maximum output power.)

3. Laser warning labels

Electrostatic discharge

Overview

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

ESD warning

NOTICE

ESD hazard

ESD can destroy electronic components.

Always keep circuit packs in antistatic covers. Use the original packaging if possible*. Use a static ground wrist strap whenever handling circuit packs or working on the Alcatel-Lucent 1665 DMX system to prevent ESD damage to sensitive components.*

All semiconductor components are basically sensitive to ESD. The ESD can also affect the components indirectly.

ESD considerations

This section describes the precautions required to prevent ESD damage.

Circuit pack handling precautions

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 ESD damage.

- Assume all circuit packs contain solid-state electronic components that can be damaged by ESD.
- When handling circuit packs (for example storing, installing, and removing) 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.
- Wear working garment made of 100% cotton to avoid ESD.
- Handle all circuit packs by the faceplate or latch and by the top and bottom outermost edges. Never touch the components, conductors, or connector pins.

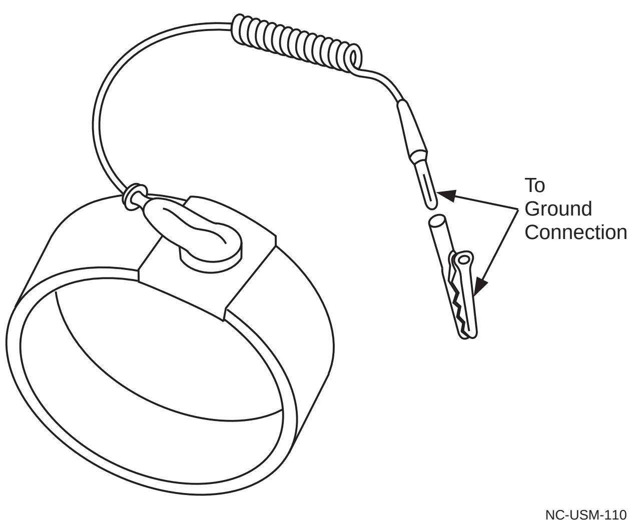
- Store and ship circuit packs and components in their shipping packing. Circuit packs and components must be packed and unpacked only at workplaces suitably protected against build-up of charge.
- Observe all warning labels on bags and cartons. Whenever possible, do not remove circuit packs from antistatic packaging until ready to insert them into slots.
- If possible, open all circuit packs at a static-safe work position, using properly grounded wrist straps and static-dissipating table mats.
- Always store and transport circuit packs 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. When removing circuit packs from a shelf, immediately place the circuit packs in static-safe packages.
- Whenever possible, maintain relative humidity above 20 percent.

Important! Ensure that any connectors on the shelf interconnection panel that are not cabled are fitted with a plastic dust cap to provide ESD protection.

Static control wrist straps

To reduce the possibility of ESD damage, the Alcatel-Lucent 1665 DMX shelf is equipped with an ESD grounding jack to enable personnel to ground themselves using wrist straps [Figure 1-2, “Static control wrist strap” (p. 1-27)], while handling circuit packs or working on the shelf. Check the wrist straps periodically with a wrist strap tester to ensure that they are working properly.

Figure 1-2 Static control wrist strap



Important! The grounding jack is located on the front of the shelf, on the lower-right corner. Another grounding jack is also located on the rear panel.

Barred-hand symbol

Circuit packs containing components that are especially sensitive to ESD are identified by warning labels bearing the barred-hand symbol. The following figure shows the barred-hand symbol.

Figure 1-3 ESD warning label (barred-hand symbol)

Save these safety instructions

READ AND UNDERSTAND ALL INSTRUCTIONS.

The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying this product.

When installing, operating, or maintaining this equipment, always follow basic safety precautions to reduce the risk of fire, electric shock, and injury to persons, including the following:

1. Read and understand all instructions.
2. Follow all warnings and instructions marked on this product.
3. Operate this product only from the type of power sources that are indicated on the marking label.
4. Connect this product only to the type of power sources recommended by Alcatel-Lucent. For information on the powering instructions, consult the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*.
5. This equipment is suitable for mounting on a concrete or other noncombustible surface only. For information on proper mounting instructions, consult the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*.
6. Install only equipment identified in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*. Use of other equipment may result in improper connection of circuitry leading to fire or injury to persons.
7. Ensure that all metallic telecommunication interfaces (traffic ports) that leave the building premises are connected to telecommunication devices that provide primary and secondary protection, as applicable.
8. Do not use this product near water; for example, in a wet basement.
9. Do not place this product on an unstable cart, stand, or table. The product may fall and cause serious damage to the product.
10. Use caution when installing or modifying telecommunications lines.
11. Never install telecommunications wiring during a lightning storm.
12. Never install telecommunications connections in wet locations.
13. Never touch uninsulated telecommunications wires or terminals unless the telecommunications line has been disconnected at the network interface.
14. Never touch uninsulated wiring or terminals carrying direct current or ringing current, and never leave this wiring exposed. Protect and tape uninsulated wiring and terminals to avoid risk of fire, electric shock, and injury to service personnel.

15. Never push objects of any kind into this product through slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electrical shock. Never spill liquids of any kind on the product.
16. To protect the unit from overheating, slots and openings in the unit are provided for ventilation. Do not block or cover these openings. Do not place this product in a built-in installation unless proper ventilation is provided.
17. To reduce the risk of an electrical shock, do not disassemble this product. Service should be performed by trained personnel only. Opening or removing covers and/or circuit boards may expose you to dangerous voltages or other risks. Incorrect reassembly can cause electrical shock when the unit is subsequently used.
18. Some of the Alcatel-Lucent 1665 DMX family hardware modules contain FDA/CDRH Class IIIb/IEC Class 1M single-mode laser products that are enclosed lightwave transmission systems.

    Under normal operating conditions, lightwave transmission systems are completely enclosed; however, the following precautions must be observed because of the potential for eye damage:

    - Do not stare directly into the optical connectors terminating the cables.
    - Ensure that technicians have satisfactorily completed an approved training course before performing lightwave/lightguide operations.
    - Do not use optical instruments such as an eye loupe to view a fiber or unterminated connector.

    More information about laser safety can be found in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*.
19. For a unit intended to be powered from −48 V DC voltage sources, read and understand the following:
    - Use only Safety Extra Low Voltage (SELV) −48 V DC sources.
    - Disconnect up to two power supply connections when removing power from the system.
    - Provide a readily accessible disconnect device as part of the building installation.
    - Ensure that there is no exposed wire when the input power cables are connected to the unit.
    - Include an independent frame ground drop to building ground. Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*.

      This electrical ground symbol is marked on the product, adjacent to the ground (earth) area for the connection of the ground (earth) conductor.
    - This equipment is to be installed only in Restricted Access Areas on Business and Customer Premises Applications in Accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA No. 70. Other installations exempt from the enforcement of the National Electrical Code may be engineered according to the accepted practices of the local telecommunications utility.

20. For a unit intended to be powered from 100-120/200-240 V AC voltage sources, read and understand the following:
    - Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
    - Do not staple or otherwise attach the power supply cord to the building surfaces.
    - Do not overload wall outlets and extension cords as this can result in the risk of fire or electrical shock.
    - Install the socket outlet near the equipment so that it is readily accessible.
    - This product is equipped with a three-wire grounding type plug, a plug having a third (grounding) pin. This plug is intended to fit only into a grounding type power outlet. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not defeat the safety purpose of the grounding type plug. Do not use a 3-to-2-prong adapter at the receptacle. Use of this type adapter may result in risk of electrical shock and/or damage to this product.
    - Do not allow anything to rest on the power cord. Do not locate this product where the cord may be abused by persons walking on it.
21. Unplug this product from the wall outlet, and refer servicing to qualified service personnel under the following conditions:
    - When the power supply cord or plug is damaged or frayed.
    - If liquid has been spilled into the product.
    - If the product has been exposed to rain or water.
    - If the product does not operate normally by following the operating instructions (Adjust only those controls that are covered by the operating instructions because improper adjustment of other controls may result in damage and will often require extensive work by qualified technician to restore the product to normal operation.)
    - If the product has been dropped or the cabinet has been damaged.
    - If the product exhibits a distinct change in performance.

SAVE THESE INSTRUCTIONS.

Eco-environmental statements

Overview

The statements that follow are the eco-environmental statements that apply to Alcatel-Lucent 1665 DMX when deployed in the European Union, China, Canada, and the United States.

Packaging collection and recovery requirements

Countries, states, localities, or other jurisdictions may require that systems be established for the return and/or collection of packaging waste from the consumer, or other end user, or from the waste stream. Additionally, reuse, recovery, and/or recycling targets for the return and/or collection of the packaging waste may be established.

For more information regarding collection and recovery of packaging and packaging waste within specific jurisdictions, please contact the Alcatel-Lucent Services - Environmental Health and Safety organization.

Material content compliance

European Union RoHS

European Union (EU) Directive 2002/95/EC, "Restriction of the use of certain Hazardous Substances" (RoHS), restricts the use of lead, mercury, cadmium, hexavalent chromium, and certain flame retardants in electrical and electronic equipment. This Directive applies to electrical and electronic products placed on the EU market after 1 July 2006, with various exemptions, including an exemption for lead solder in network infrastructure equipment. Alcatel-Lucent products shipped to the EU after 1 July 2006 comply with the EU RoHS Directive.

China RoHS

The Peoples Republic of China Ministry of Information Industry has published a regulation (Order #39) and associated standards regarding restrictions on hazardous substances (China RoHS). Currently, the legislation requires all Electronic and Information Products (EIP) to comply with certain labeling and documentation requirements. Alcatel-Lucent products manufactured on or after 1 March 2007, that are intended for sale to customers in the China market, comply with these requirements.

In accordance with the People's Republic of China Electronic Industry Standard "Marking for the Control of Pollution Caused by Electronic Information Product" (SJ/T11364- 2006), customers may access Alcatel-Lucent's Hazardous Substances Table information at either of the following two URLs (for the convenience of our diverse customer base):

- Access via the Alcatel-Lucent Corporate website at:

http://www.alcatel-sbell.com.cn/live/home/index.jsp (http://www.alcatel-sbell.com.cn/live/home/index.jsp)

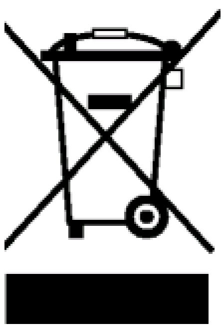
- Access via the Alcatel Shanghai Bell website at:

  http://www.alcatel-sbell.com.cn/wwwroot/images/upload/private/1/media/China-RoHS-HST-3.1.pdf (http://www.alcatel-sbell.com.cn/wwwroot/images/upload/private/1/media/China-RoHS-HST-3.1.pdf)

Recycling / take-back / disposal of products

Electronic products bearing or referencing the symbols shown below shall be collected and treated at the end of their useful life, in compliance with applicable European Union and other local legislation. They shall not be disposed of as part of unsorted municipal waste. Due to materials that may be contained in the product and batteries, such as heavy metals, the environment and human health may be negatively impacted as a result of inappropriate disposal.

Note: For electronic products put on the market in the European Union, a solid bar under the crossed-out wheeled bin indicates that the product was put on the market after 13 August 2005.



Moreover, in compliance with legal requirements and contractual agreements, where applicable, Alcatel-Lucent will offer to provide for the collection and treatment of Alcatel-Lucent products bearing the logo at the end of their useful life, or products displaced by Alcatel-Lucent equipment offers.

For information regarding take-back, recycling, or disposal of equipment by Alcatel-Lucent or for equipment take-back requests, visit the Alcatel-Lucent Take-Back web page (http://www.alcatel-lucent.com/product_takeback) or contact Alcatel-Lucent Takeback Support (takeback@alcatel-lucent.com). For technical information on product treatment, consult the Alcatel-Lucent Recycling Information web page (http://www.alcatel-lucent.com/product_recycling).

2 Alarm list

Overview

Purpose

This chapter contains the alarm list for the Alcatel-Lucent 1665 Data Multiplexer.

Contents

Alarm list with severity levels

Overview

This section provides the reported alarm list with severity levels.

Alarm list

Important! The severity level for certain alarms is provisionable. In the table below, a bold **X** identifies the default severity level for alarm messages that have provisionable severity levels. If there are multiple severity levels listed, yet there is no bold **X**, the severity level for that alarm or condition is determined by equipment provisioning.

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`-48V power/ fuse FA failed`	PWR	X	X	X	**X**	X	Procedure 5-2: " Clear "−48V power/fuse FA or FB failed" alarm" (p. 5-13)
`-48V power/ fuse FB failed`	PWR	X	X	X	**X**	X	
`ABN condition`	MAN					X[2]	Locate the corresponding Not Alarmed (SC) in the alarm list and proceed to the appropriate procedure to release/clear the condition.
`ACO active`	INHAUDB					X	No action is necessary.
`AGNE communication failure`	PRCDRERR	X	X	**X**	X	X	Procedure 5-3: "Clear "AGNE communication failure" alarm" (p. 5-18)
`AUTO link shutdown`	ALS	X	X	X	X	**X**[2]	Procedure 5-5: "Clear "AUTO link shutdown" alarm" (p. 5-24)
`automatic lock`	WKSWPR-1 WKSWPR-2					X[2]	Procedure 5-6: "Clear "automatic lock" condition" (p. 5-26)
`Automatic protection switch mode mismatch`	APSMM	X	X	**X**	X	X	Procedure 5-7: "Clear "Automatic protection switch mode mismatch" alarm" (p. 5-29)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
Automatic protection switch primary section mismatch	APSPSM	X	X	X	X	X	Procedure 5-8: "Clear "Automatic protection switch primary section mismatch" alarm" (p. 5-31)
Automatic protection switch unused codes	APSUC	X	X	X	X	X	Procedure 5-9: "Clear "Automatic protection switch unused codes" alarm" (p. 5-34)
Automatic protection switch unresolved transient codes	APSUT	X	X	X	X	X	Procedure 5-10: "Clear "Automatic protection switch unresolved transient codes" alarm" (p. 5-36)
Circuit Provisioning Error	PAPRVERR	X	X	X	X	X	Procedure 5-12: "Clear "Circuit Provisioning Error" alarm" (p. 5-43)
copy program IP	EOC					X	No action is necessary.
CP contributing to a pack failure	CTNEQPT	X	X	X	X	X	Procedure 5-13: "Clear "CP failed/CP contributing to a pack failure" alarms" (p. 5-44)
CP initialization IP	FACTERM					X	No action is necessary.
CP not allowed - crs	FACTERM	X	X	X	X[6]	X	Procedure 5-14: "Clear "CP not allowed - crs" alarm" (p. 5-49)
CP not allowed - eqpt	FACTERM	X	X	X	X[6]	X	Procedure 5-15: "Clear "CP not allowed - eqpt" alarm" (p. 5-51)
CP removed or CP failure	FACTERM	X	X[5]	X	X[6]	X	Procedure 5-16: "Clear "CP removed or CP failure" alarm" (p. 5-53)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`CP software upgrade required`	FACTERM					X	Procedure 5-17: "Clear "CP software upgrade required" condition" (p. 5-55)
`CPY-MEM backup IP`	EOC					X	No action is necessary.
`CPY-MEM download IP`	EOC					X	
`CPY-MEM restore IP`	EOC					X	
`DATA CP failed`	FACTERM	X	X	X	X	X	Procedure 5-13: "Clear "CP failed/CP contributing to a pack failure" alarms" (p. 5-44)
`DATA terminal loopback`	LPBKNETWORK					X[2]	Procedure 5-18: "Clear "DATA terminal loopback" condition" (p. 5-57)
`Default K-bytes`	BLSR-DKB	X	X	X	X	X	Procedure 5-19: "Clear "Default K-bytes" alarm" (p. 5-58)
`dormant/exec code mismatch`	EOC					X	Procedure 5-20: "Clear "dormant/exec code mismatch" condition" (p. 5-61)
`DS1 CP failed`	FACTERM	X	X[5]	X	X[6]	X	Procedure 5-13: "Clear "CP failed/CP contributing to a pack failure" alarms" (p. 5-44)
`DS1E1 CP failed`	FACTERM	X	X[5]	X	X[6]	X	Procedure 5-13: "Clear "CP failed/CP contributing to a pack failure" alarms" (p. 5-44)
`DS1 loopback (to DSX)`	LPBKNETWORK					X[2]	Procedure 5-21: "Clear "DS1 loopback (to DSX)" condition" (p. 5-62)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
DS1 loopback (to Fiber)	LPBKNETWORK					X[2]	Procedure 5-22: “Clear "DS1 loopback (to Fiber)" condition” (p. 5-63)
DS1 trmsn test IP	LPBKNETWORK					X[2]	No action is necessary.
DS3 loopback (to DSX)	LPBKNETWORK					X[2]	Procedure 5-23: “Clear "DS3 loopback (to DSX)" condition” (p. 5-64)
DS3 loopback (to Fiber)	LPBKNETWORK					X[2]	Procedure 5-24: “Clear "DS3 loopback (to Fiber)" condition” (p. 5-65)
DS3 trmsn test IP	LPBKNETWORK					X[2]	No action is necessary.
DS3EC1 CP failed	FACTERM	X	X[5]	X	X[6]	X	Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44)
Duplicate Ring Node	DUPL-RNG	X	X	X	X	X	Procedure 5-25: “Clear "Duplicate Ring Node" alarm” (p. 5-66)
E1 loopback (to DSX)	LPBKNETWORK					X[2]	Procedure 5-26: “Clear "E1 loopback (to DSX)" condition” (p. 5-68)
E1 loopback (to Fiber)	LPBKNETWORK					X[2]	Procedure 5-27: “Clear "E1 loopback (to Fiber)" condition” (p. 5-69)
E1 trmsn test IP	LPBKNETWORK					X[2]	No action is necessary.
EC1 loopback (to DSX)	LPBKNETWORK					X[2]	Procedure 5-28: “Clear "EC1 loopback (to DSX)" condition” (p. 5-70)
EC1 loopback (to Fiber)	LPBKNETWORK					X[2]	Procedure 5-29: “Clear "EC1 loopback (to Fiber)" condition” (p. 5-71)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`ECV - excessive code violation`	ECV	X	X	X	X	X	Procedure 5-30: "Clear "ECV - excessive code violation" alarm" (p. 5-72)
`ENET facility loopback`	LPBKNETWORK					X[2]	Procedure 5-31: "Clear "ENET loopback" conditions" (p. 5-77)
`ENET terminal loopback`	LPBKNETWORK					X[2]	
`ENNI signaling communication failure with peer`	SIGPEER	X	X	X	X	X	Procedure 5-32: "Clear "ENNI signaling communication failure with peer" alarm" (p. 5-78)
`environmentn`	MISC		X	X	X	X	Procedure 5-33: "Clear "environmentn" alarm" (p. 5-82)
`Equipment configuration no longer supported`	DATAFLT				X		Procedure 5-44: "Clear "Generic/Database/Equipment Configuration" alarms/conditions" (p. 5-104)
`ERP - Multiple RPL Owners`	ERP-MO	X	X	X	X	X	Procedure 5-34: "Clear "ERP - Multiple RPL Owners" alarm" (p. 5-83)
`ERP - PDU Watchdog Timeout`	ERP-WD	X	X	X	X	X	Procedure 5-35: "Clear "ERP - PDU Watchdog Timeout" alarm" (p. 5-85)
`Exceeded MTU size drop`	EMSD	X	X	X	X	X	Procedure 5-36: "Clear "Exceeded MTU size drop" alarm" (p. 5-88)
`excessive holdover`	LHI	X	X	X	X	X	Procedure 5-45: "Clear "holdover" conditions/alarms" (p. 5-113)
`Excessive Reserved Rate on RPR`	EXS-RSV					X[2]	Procedure 5-37: "Clear "Excessive Reserved Rate on RPR" condition" (p. 5-90)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`Extra Traffic Preempted`	RNG-PREEMPT					X[2]	Procedure 5-38: "Clear "Extra Traffic Preempted" condition" (p. 5-93)
`fan shelf failed`	EXT		X	X	X	X	Procedure 5-39: "Clear "fan shelf failed" alarm" (p. 5-95)
`far end not LCAS`	NOTLCAS					X	Procedure 5-40: "Clear "far end not LCAS" condition" (p. 5-99)
`Far-end protection line failure`	FEPRLF	X	X	X	X	X	Procedure 5-41: "Clear "Far-end protection line failure" alarm" (p. 5-101)
`FE-LAN CP failed`	FACTERM	X	X	X	X	X	Procedure 5-13: "Clear "CP failed/CP contributing to a pack failure" alarms" (p. 5-44)
`forced switch`	WKSWPR-1 WKSWPR-2					X[2]	Procedure 5-42: "Clear "forced switch" condition" (p. 5-102)
`Forced Switch`	FSR					X[2]	Procedure 5-43: "Clear "Forced Switch" condition" (p. 5-103)
`GE-LAN CP failed`	FACTERM	X	X	X	X	X	Procedure 5-13: "Clear "CP failed/CP contributing to a pack failure" alarms" (p. 5-44)
`generic validation IP`	EOC					X	No action is necessary.
`holdover mode active`	HLDOVRSYNC					X	Procedure 5-45: "Clear "holdover" conditions/alarms" (p. 5-113)
`illegal CP type`	FACTERM	X[5]	X	X	X[6]	X	Procedure 5-46: "Clear "illegal CP type" alarm" (p. 5-115)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`Improper APS Codes`	APSPROV	X	X	X	X	X	Procedure 5-47: "Clear "Improper APS Codes" alarm" (p. 5-117)
`inc. data type mismatch`	MISC					X	Procedure 5-48: "Clear "inc. data type mismatch" alarm" (p. 5-121)
`inc. DS1 sync. ref. AIS`	SYNC	X	X	X	X	X	Procedure 5-49: "Clear "inc. DS1/E1 sync. ref." alarms" (p. 5-125)
	SYNCOOS	X	X	X	X	X	
`inc. DS1 sync. ref. BER`	SYNC	X	X	X	X	X	
	SYNCOOS	X	X	X	X	X	
`inc. DS1 sync. ref. EOOF`	SYNC	X	X	X	X	X	
	SYNCOOS	X	X	X	X	X	
`inc. DS1 sync. ref. LOF`	SYNC	X	X	X	X	X	
	SYNCOOS	X	X	X	X	X	
`inc. DS1 sync. ref. LOS`	SYNC	X	X	X	X	X	
	SYNCOOS	X	X	X	X	X	
`inc. DS1 sync. ref. OOL`	SYNC	X	X	X	X	X	
	SYNCOOS	X	X	X	X	X	
`inc. DS3 Cbit Mismatch`	CBITMM	X	X	X	X	X	Procedure 5-52: "Clear "inc. DS3 Cbit Mismatch" alarm" (p. 5-134)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
inc. E1 sync. ref. AIS	SYNC	X	X	X	X	X	Procedure 5-49: "Clear "inc. DS1/E1 sync. ref." alarms" (p. 5-125)
	SYNCOOS	X	X	X	X	X	
inc. E1 sync. ref. BER	SYNC	X	X	X	X	X	
	SYNCOOS	X	X	X	X	X	
inc. E1 sync. ref. CRC-4 MFA mismatch	SYNC	X	X	X	X	X	
	SYNCOOS	X	X	X	X	X	
inc. E1 sync. ref. LOF	SYNC	X	X	X	X	X	
	SYNCOOS	X	X	X	X	X	
inc. E1 sync. ref. LOS	SYNC	X	X	X	X	X	
	SYNCOOS	X	X	X	X	X	
inc. E1 sync. ref. OOL	SYNC	X	X	X	X	X	
	SYNCOOS	X	X	X	X	X	
inc. (from DSX) DS1 AIS	AIS	X	X	X	X	X	Procedure 5-50: "Clear "inc. (from DSX) DS1" alarms" (p. 5-128)
inc. (from DSX) DS1 LOF	LOF	X	X	X	X	X	
inc. (from DSX) DS1 LOS	LOS	X	X	X	X	X	
inc. (from DSX) DS1 RAI	RAI	X	X	X	X	X	Procedure 5-53: "Clear "inc. (from DSX) DSn RAI" alarm" (p. 5-137)
inc. (from DSX) DS1 sig. failed	T-BERL	X	X	X	X	X	Procedure 5-50: "Clear "inc. (from DSX) DS1" alarms" (p. 5-128)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`inc. (from DSX) DS3 AIS`	AIS	X	X	X	X	X	Procedure 5-51: "Clear "inc. (from DSX) DS3" alarms" (p. 5-131)
`inc. (from DSX) DS3 IDLE`	IDLE	X	X	X	X	X	
`inc. (from DSX) DS3 LOF`	LOF	X	X	X	X	X	
`inc. (from DSX) DS3 LOS`	LOS	X	X	X	X	X	
`inc. (from DSX) DS3 RAI`	RAI	X	X	X	X	X	Procedure 5-53: "Clear "inc. (from DSX) DSn RAI" alarm" (p. 5-137)
`inc. (from DSX) DS3 sig. failed`	T-BERL	X	X	X	X	X	Procedure 5-51: "Clear "inc. (from DSX) DS3" alarms" (p. 5-131)
`inc. (from fiber) DS1 AIS`	AIS-EGR	X	X	X	X	X	Procedure 5-54: "Clear "inc. (from fiber) DSn" alarms" (p. 5-139)
`inc. (from fiber) DS1 LOF`	LOF-EGR	X	X	X	X	X	
`inc. (from fiber) DS1 RAI`	RAI-EGR	X	X	X	X	X	Procedure 5-55: "Clear "inc. (from fiber) DSn RAI" alarms" (p. 5-141)
`inc. (from fiber) DS3 AIS`	AIS-EGR	X	X	X	X	X	Procedure 5-54: "Clear "inc. (from fiber) DSn" alarms" (p. 5-139)
`inc. (from fiber) DS3 LOF`	LOF-EGR	X	X	X	X	X	
`inc. (from fiber) DS3 RAI`	RAI-EGR	X	X	X	X	X	Procedure 5-55: "Clear "inc. (from fiber) DSn RAI" alarms" (p. 5-141)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`inc. (from DSX) E1 AIS`	AIS	X	X	X	X	X	Procedure 5-56: “Clear "inc. (from DSX) E1" alarms” (p. 5-142)
`inc. (from DSX) E1 LOF`	LOF	X	X	X	X	X	
`inc. (from DSX) E1 LOS`	LOS	X	X	X	X	X	
`inc. (from DSX) E1 sig. failed`	T-BERL	X	X	X	X	X	
`inc. EC1 line AIS`	AIS	X	X	X	X	X	Procedure 5-57: “Clear "inc. EC1" alarms” (p. 5-145)
`inc. EC1 LOF`	LOF	X	X	X	X	X	
`inc. EC1 LOS`	LOS	X	X	X	X	X	
`inc. EC1 RFI-L`	FERF	X	X	X	X	X	
`inc. EC1 section trace identifier mismatch`	TIM-S	X	X	X[5]	X[6]	X	Procedure 5-73: “Clear "inc. section trace identifier mismatch" alarms” (p. 5-192)
`inc. EC1 section trace identifier mismatch, diagnostic`	TIM-S-D	X	X	X	X	X	
`inc. EC1 sig. degrade (BER)`	T-BERL	X	X	X	X	X	Procedure 5-57: “Clear "inc. EC1" alarms” (p. 5-145)
`inc. EC1 sig. failed (BER)`	T-BERL	X	X	X	X	X	
`inc. FE-LAN ANM`	ANM	X	X	X	X	X	Procedure 5-58: “Clear "inc. FE-LAN ANM" alarm” (p. 5-147)
`inc. FE-LAN FEFI`	FERF	X	X	X	X	X	Procedure 5-59: “Clear "inc. FE-LAN FEFI" alarm” (p. 5-151)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`inc. FE-LAN LOS`	LOS	X	X	X	X	X	Procedure 5-60: "Clear "inc. FE-LAN LOS" alarm" (p. 5-154)
`inc. GE-LAN ANM`	ANM	X	X[5]	X	X[6]	X	Procedure 5-61: "Clear "inc. GE-LAN ANM" alarm" (p. 5-156)
`inc. GE-LAN LOS`	LOS	X	X[5]	X	X[6]	X	Procedure 5-62: "Clear "inc. GE-LAN LOS" alarm" (p. 5-159)
`inc. LAG Partial Link Loss`	PLL	X	X	X	X	X	Procedure 5-64: "Clear "inc. LAG" alarms" (p. 5-164)
`inc. LAG PLCF`	PLCF	X	X	X	X	X	
`inc. LAG Total Link Loss`	TLL	X	X	X	X	X	
`inc. line sync. ref. OOL`	SYNC	X	X	X	X	X	Procedure 5-63: "Clear "inc. line sync. ref. OOL" alarm" (p. 5-161)
	SYNCOOS	X	X	X	X	X	
`inc. LOS`	LOS	X	X[5]	X	X[6]	X	Procedure 5-65: "Clear "inc. LOS" alarm" (p. 5-168)
`inc. Loss of Synch`	LSYNC	X	X[5]	X	X[6]	X	Procedure 5-66: "Clear "inc. Loss of Synch" alarm" (p. 5-170)
`inc. MUX OCH LOS-P`	MUX-LOS-P	X	X	X	X	X	Procedure 5-67: "Clear "inc. MUX OCH LOS-P" alarm" (p. 5-172)
`inc. OCN line AIS`	AIS	X	X[5]	X	X	X[6]	Procedure 5-68: "Clear "inc. OCN" alarms" (p. 5-176)
`inc. OCN LOF`	LOF	X	X[5]	X	X[6]	X	
`inc. OCN LOS`	LOS	X	X[5]	X	X[6]	X	
`inc. OCN RFI-L`	FERF	X	X	X	X	X	Procedure 5-69: "Clear "inc. OCN RFI-L" alarm" (p. 5-180)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`inc. OCN section trace identifier mismatch`	TIM-S	X	X	X[5]	X[6]	X	Procedure 5-73: "Clear "inc. section trace identifier mismatch" alarms" (p. 5-192)
`inc. OCN section trace identifier mismatch, diagnostic`	TIM-S-D	X	X	X	X	X	
`inc. OCN sig. degrade (BER)`	T-BERL	X	X[5]	X	X[6]	X	Procedure 5-68: "Clear "inc. OCN" alarms" (p. 5-176)
`inc. OCN sig. failed (BER)`	T-BERL	X	X[5]	X	X[6]	X	
`inc. ODU2 BDI`	BDI	X	X	X	X	X[6]	Procedure 5-11: "Clear "inc. BDI" alarms" (p. 5-38)
`inc. ODU2 DEG`	DEG	X	X[5]	X	X[6]	X	Procedure 5-71: "Clear "inc. ODU2/OTU2" alarms" (p. 5-185)
`inc. ODU2 LCK`	LCK	X	X[5]	X	X[6]	X	Procedure 5-70: "Clear "inc. ODU2 LCK/OCI" alarms" (p. 5-184)
`inc. ODU2 OCI`	OCI	X	X[5]	X	X[6]	X	
`inc. ODU2 SSF`	SSF	X	X[5]	X	X[6]	X	Procedure 5-71: "Clear "inc. ODU2/OTU2" alarms" (p. 5-185)
`inc. OTS LOS-P`	LOS-P	X	X[5]	X	X[6]	X	Procedure 5-72: "Clear "inc. OTS LOS-P" alarm" (p. 5-189)
`inc. OTU2 BDI`	BDI	X	X	X	X	X[6]	Procedure 5-11: "Clear "inc. BDI" alarms" (p. 5-38)
`inc. OTU2 DEG`	DEG	X	X[5]	X	X[6]	X	Procedure 5-71: "Clear "inc. ODU2/OTU2" alarms" (p. 5-185)
`inc. OTU2 LOF`	LOF	X	X[5]	X	X[6]	X	
`inc. OTU2 LOM`	LOM	X	X[5]	X	X[6]	X	
`inc. OTU2 LOS-P`	LOS-P	X	X[5]	X	X[6]	X	
`inc. OTU2 SSF`	SSF	X	X[5]	X	X[6]	X	

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`inc. STS LOP`	LOP	X	X[5]	X	X[6]	X	Procedure 5-57: "Clear "inc. EC1" alarms" (p. 5-145)
`inc. STSN`[3] `AIS`	AIS	X	X[5]	X	X[6]	X	Procedure 5-74: "Clear "inc. STSN" conditions/alarms" (p. 5-195)
`inc. STSN LOP`	LOP	X	X[5]	X	X[6]	X	
`inc. STSN RFI-P`	YEL	X	X	X	X	X	
`inc. STSN sig. degrade (BER)`	T-BERP	X	X[5]	X	X[6]	X	
`inc. STSN sig. failed (BER)`	T-BERP	X	X[5]	X	X[6]	X	
`inc. STSN unequipped`	SLMF	X	X[5]	X	X[6]	X	
`inc. VCG failed`	LOS	X	X[5]	X	X[6]	X	Procedure 5-75: "Clear "inc. VCG failed" alarm" (p. 5-199)
`inc. VCG LFD`	MISC					X	Procedure 5-76: "Clear "inc. VCG LFD" condition" (p. 5-203)
`inc. VCG LOA`	MISC					X	Procedure 5-77: "Clear "inc. VCG LOA" condition" (p. 5-206)
`inc. VC TU-AIS`	AIS	X	X	X	X	X	Procedure 5-78: "Clear "inc. VC" conditions/alarms" (p. 5-208)
`inc. VC TU-LOP`	LOP	X	X	X	X	X	
`inc. VC LP-RFI`	YEL	X	X	X	X	X	
`inc. VC unequipped`	SLMF	X	X	X	X	X	
`inc. VT AIS`	AIS	X	X	X[5]	X[6]	X	Procedure 5-79: "Clear "inc. VT" conditions/alarms" (p. 5-212)
`inc. VT LOP`	LOP	X	X	X[5]	X[6]	X	
`inc. VT RFI-V`	YEL	X	X	X	X	X	
`inc. VT sig. degrade (BER)`	T-BERP	X	X	X[5]	X[6]	X	
`inc. VT unequipped`	SLMF	X	X	X[5]	X[6]	X	

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`incoming CRC-4 MFA mismatch`	CRCMM	X	X	X	X	X	Procedure 5-80: "Clear "incoming CRC-4 MFA mismatch" condition" (p. 5-216)
`incompatible CP version`	FACTERM	X	X	X	X	X	Procedure 5-81: "Clear "incompatible CP version" alarm" (p. 5-218)
`Inconsistent APS Codes`	APSC	X	X	X	X	X	Procedure 5-82: "Clear "Inconsistent APS Codes" alarm" (p. 5-219)
`Inconsistent crs map`	CONTR				X		Procedure 5-83: "Clear "Inconsistent crs map" alarm" (p. 5-223)
`inconsistent DCC values`	OSILINKERR	X	X	X	X	X	Procedure 5-84: "Clear "inconsistent DCC values" alarm" (p. 5-224)
`Inconsistent Ring Prot Mode`	RNG-IRPM	X	X	X	X	X	Procedure 5-85: "Clear "Inconsistent Ring Prot Mode" alarm" (p. 5-226)
`Inconsistent VT BLSR Access`	RNG-IVTBA					X[2]	Procedure 5-86: "Clear "Inconsistent VT BLSR Access" condition" (p. 5-227)
`inhibit switch`	INHSWPR WKSWPR-1 WKSWPR-2	X	X	X	X	X[2]	Procedure 5-87: "Clear "inhibit switch" condition" (p. 5-230)
`install failed`	FACTERM					X[2]	Procedure 5-88: "Clear "install failed" condition" (p. 5-231)
`install program IP`	EOC SWFTDWN					X	No action is necessary.

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`Invalid Database`	DATAFLT			X			Procedure 5-44: "Clear "Generic/Database/Equipment Configuration" alarms/conditions" (p. 5-104)
`Invalid Subshelf Configuration`	DATAFLT				X		Procedure 5-135: "Clear "Subshelf-related" alarms/conditions" (p. 5-329)
`Line Automatic Switch`	LAS					X[2]	Procedure 5-89: "Clear "Line Automatic Switch" condition" (p. 5-234)
`line DCC channel failed`	EOC-L	X	X	X	X	X	Procedure 5-90: "Clear "line DCC channel failed" alarm" (p. 5-237)
`lockout of protection`	INHSWPR					X[2]	Procedure 5-91: "Clear "lockout of protection" condition" (p. 5-243)
`Lockout Switch`	LPS					X[2]	Procedure 5-92: "Clear "Lockout Switch" condition" (p. 5-244)
`lockout switching`	GP					X[2]	Procedure 5-93: "Clear "lockout switching" condition" (p. 5-245)
`Maintenance Mode`	DATAFLT					X[2]	Procedure 5-44: "Clear "Generic/Database/Equipment Configuration" alarms/conditions" (p. 5-104)
`manual reference switch`	WKSWPR-1 WKSWPR-2					X[2]	Procedure 5-94: "Clear "manual reference switch" condition" (p. 5-246)
`manual switch`	WKSWPR-1 WKSWPR-2 MSR					X[2]	Procedure 5-95: "Clear "manual switch" condition" (p. 5-247)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`Manual Switch`	MSR					X[2]	Procedure 5-96: "Clear "Manual Switch" condition" (p. 5-249)
`manual sync. mode switch`	HLDOVRSYNC					X[2]	Procedure 5-97: "Clear "manual sync. mode switch" condition" (p. 5-250)
`Member Not Collecting/ Distributing`	MNCD	X	X	X	X	X	Procedure 5-98: "Clear "Member Not Collecting/Distributing" alarm" (p. 5-251)
`Member Signal Unacceptable - LCAS`	MSU-L	X	X	X	X[5,6]	X	Procedure 5-99: "Clear "Member Signal Unacceptable - LCAS" alarm" (p. 5-253)
`Multiple Databases`	DATAFLT			X			Procedure 5-44: "Clear "Generic/Database/Equipment Configuration" alarms/conditions" (p. 5-104)
`Multiple Generics`	DATAFLT			X			Procedure 5-44: "Clear "Generic/Database/Equipment Configuration" alarms/conditions" (p. 5-104)
`Multiple Main Shelf TIDs`	DATAFLT				X		Procedure 5-135: "Clear "Subshelf-related" alarms/conditions" (p. 5-329)
`Muxponder CP failed`	FACTERM	X	X[5]	X	X	X	Procedure 5-13: "Clear "CP failed/CP contributing to a pack failure" alarms" (p. 5-44)
`neighbor SYSCTL CP unavailable` (nbr tid = *TID*)	CONTR	X	X	X	X	X	Procedure 5-100: "Clear "neighbor SYSCTL CP unavailable (nbr tid = TID)" alarm" (p. 5-257)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`Node ID Mismatch`	NID-CONFL	X	X	X	X	X	Procedure 5-101: "Clear "Node ID Mismatch" alarm" (p. 5-260)
`NP audit failed`	NPAUDT	X	X[5]	X	X[6]	X	Procedure 5-4: "Clear "audit failed" alarms" (p. 5-21)
`NSAP count in L1 overflowed`	BUFROVLD	X	X	X	X	X	Procedure 5-102: "Clear "NSAP count in L1 overflowed" alarm" (p. 5-264)
`NSAP count in L1 threshold crossed`	BUFROVLD	X	X	X	X	X	Procedure 5-103: "Clear "NSAP count in L1 threshold crossed" alarm" (p. 5-265)
`NTP server(s) unreachable`	EOC					X	Procedure 5-104: "Clear "NTP server(s) unreachable" condition" (p. 5-266)
`NUT Inconsistent XC Granularity`	NUTINXCGRN	X	X	X	X	X	Procedure 5-105: "Clear "NUT Inconsistent XC Granularity" alarm" (p. 5-267)
`NVM failed`	WKGMEM	X[7]	X	X	X		Procedure 5-106: "Clear "NVM" alarms" (p. 5-269)
`NVM removed or NVM failed`	WKGMEM	X[7]	X	X	X		Procedure 5-106: "Clear "NVM" alarms" (p. 5-269)
`NVM write disabled`	WKGMEM					X[2]	No action is necessary.
`OCN facility loopback`	LPBKNETWORK					X[2]	Procedure 5-107: "Clear "OCN facility loopback" condition" (p. 5-274)
`OCN terminal loopback`	LPBKNETWORK					X[2]	Procedure 5-108: "Clear "OCN terminal loopback" condition" (p. 5-275)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
OLIU CP failed	FACTERM	X	X[5]	X	X[6]	X	Procedure 5-13: "Clear "CP failed/CP contributing to a pack failure" alarms" (p. 5-44)
OMD CP failed	FACTERM	X	X[5]	X	X	X	
Path Integrity Failure	PAINTGRT	X	X	X	X	X	Procedure 5-112: "Clear "Path Integrity Failure" alarm" (p. 5-281)
Pluggable Transmission Module insufficient maximum rate	FACTERM	X	X[5]	X	X[6]	X	Procedure 5-109: "Clear "Pluggable Transmission Module insufficient maximum rate" alarm" (p. 5-276)
Pluggable Transmission Module maintenance IP	MAN					X[2]	Procedure 5-110: "Clear "Pluggable Transmission Module maintenance IP" condition" (p. 5-278)
Pluggable Transmission Module removed	FACTERM	X	X[5]	X	X[6]	X	Procedure 5-111: "Clear "Pluggable Transmission Module removed" alarm" (p. 5-279)
Port administratively	MAN disabled					X[2]	Procedure 5-113: "Clear "Port administratively disabled" condition" (p. 5-282)
Protection CP Input fault	FACTERM	X	X	X	X	X	Procedure 5-116: "Clear "PROTN Port Failure/Protection CP Input fault" alarms" (p. 5-287)
Protection switching byte failure	APSB	X	X	X	X	X	Procedure 5-114: "Clear "Protection switching byte failure" alarm" (p. 5-283)
Protection switching channel match failure	APSCM	X	X	X	X	X	Procedure 5-115: "Clear "Protection switching channel match failure" alarm" (p. 5-285)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
PROTN DS3 Port Failure	PROTNA	X	X	X	X	X	Procedure 5-116: “Clear "PROTN Port Failure/Protection CP Input fault" alarms” (p. 5-287)
PROTN EC1 Port Failure	PROTNA	X	X	X	X	X	
Receive buffer overflow	BUFROVLD					X[2]	Procedure 5-117: “Clear "Receive buffer overflow" condition” (p. 5-290)
Remote client signal failed	GFP_RCF	X	X[5]	X	X[6]	X	Procedure 5-118: “Clear "Remote client signal failed" alarm” (p. 5-292)
remote install/ copy program IP	EOC					X	No action is necessary.
Ring Circuit Alarm Suppressed	CKTAUDUD					X[2]	Procedure 5-119: “Clear "Ring Circuit Alarm Suppressed" condition” (p. 5-295)
Ring Ckt Validation Suspended	CKTAUDSNP	X	X	X	X	X	Procedure 5-120: “Clear "Ring Ckt Validation Suspended" alarm” (p. 5-296)
Ring Comm Failure	RNG-DSCVY	X	X	X	X	X	Procedure 5-121: “Clear "Ring Comm Failure" alarm” (p. 5-298)
Ring Discovery In Progress	RNG-DSCVY					X[2]	No action is necessary.
Ring Incomplete	RNG-INC	X	X	X	X	X	Procedure 5-122: “Clear "Ring Incomplete" alarm” (p. 5-301)
Ring Prot Switching Suspended	OVRDSW	X	X	X	X	X	Procedure 5-123: “Clear "Ring Prot Switching Suspended" alarm” (p. 5-307)
ring upgrade mode	RINGUPGRADE					X[2]	Procedure 5-124: “Clear "ring upgrade mode" condition” (p. 5-309)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
RPR Miscabling	MISCBL					X[2]	Procedure 5-125: "Clear "RPR Miscabling" condition" (p. 5-310)
RPR Topology Exceeded Max Stations	TOPO-MAX					X[2]	Procedure 5-126: "Clear "RPR Topology Exceeded Max Stations" condition" (p. 5-312)
RPR Topology Inconsistency	TOPO-INCS					X[2]	Procedure 5-127: "Clear "RPR Topology Inconsistency" condition" (p. 5-313)
RPR Topology Map Entry Invalid	TOPO-INV					X[2]	Procedure 5-128: "Clear "RPR Topology Map Entry Invalid" condition" (p. 5-315)
RPR Topology Unstable	TOPO-UNST					X[2]	Procedure 5-129: "Clear "RPR Topology Unstable" condition" (p. 5-316)
section DCC channel failed	EOC	X	X	X	X	X	Procedure 5-130: "Clear "section DCC channel failed" alarm" (p. 5-317)
Segment audit failed LAN in	SEGAUDTIN	X	X	X	X	X	Procedure 5-4: "Clear "audit failed" alarms" (p. 5-21)
Segment audit failed LAN out	SEGAUDTOUT	X	X	X	X	X	
Segment audit failed VCG in	SEGAUDTIN	X	X	X	X	X	
Segment audit failed VCG out	SEGAUDTOUT	X	X	X	X	X	
Squelch Map Inconsistent	SQMAP-INCST	X	X	X	X	X	Procedure 5-131: "Clear "Squelch Map Inconsistent" alarm" (p. 5-321)
Squelch Data Unavailable	SQDATA-UNAV	X	X	X	X	X	Procedure 5-132: "Clear "Squelch Data Unavailable" alarm" (p. 5-322)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`STP autolock port disable`	AUTOLOCK	X	X	X	X	X	Procedure 5-133: "Clear "STP autolock port disable" alarm" (p. 5-324)
`Subshelf Boot Failed`	DATAFLT				X		Procedure 5-135: "Clear "Subshelf-related" alarms/conditions" (p. 5-329)
`Subshelf Communication Failed`	REMLINK	X	X	X	X	X	Procedure 5-134: "Clear "Subshelf Communication Failed" alarm" (p. 5-326)
`Subshelf Configuration Mismatch`	DATAFLT				X		Procedure 5-135: "Clear "Subshelf-related" alarms/conditions" (p. 5-329)
`Subshelf initialization IP`	EOC	X	X	X	X	X	No action is necessary.
`SYSCTL CP failed`	CONTR	X	X	X	X	X	Procedure 5-13: "Clear "CP failed/CP contributing to a pack failure" alarms" (p. 5-44)
`SYS dorm area corrupted`	EOC					X	Procedure 5-136: "Clear "SYS dorm area corrupted" condition" (p. 5-339)
`SYS generic corrupted`	EOC		X	X	X	X	Procedure 5-137: "Clear "SYS generic corrupted" alarm" (p. 5-340)
`SWITCH CP failed`	FACTERM	X	X	X	X	X	Procedure 5-13: "Clear "CP failed/CP contributing to a pack failure" alarms" (p. 5-44)
`Temporarily NUT Provisioned`	NUTTMPPRV					X	Procedure 5-138: "Clear "Temporarily NUT Provisioned" condition" (p. 5-342)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`Test access IP`	TSTACC					X[2]	Procedure 5-139: "Clear "Test access IP" conditions" (p. 5-343)
`Test access IP:` *tsn*	TSTACC					X[2]	
`time of day not provisioned`	CONTR					X	Procedure 5-140: "Clear "time of day not provisioned" condition" (p. 5-344)
`TMUX CP failed`	FACTERM	X	X[5]	X	X[6]	X	Procedure 5-13: "Clear "CP failed/CP contributing to a pack failure" alarms" (p. 5-44)
`Traffic Squelched`	RNG-SQUELCH					X	Procedure 5-141: "Clear "Traffic Squelched" condition" (p. 5-346)
`unexpected circuit pack type`	FACTERM					X[2]	No action is necessary.
`unexpected CP type`	FACTERM	X	X[5]	X	X[6]	X	Procedure 5-142: "Clear "unexpected CP type" alarm" (p. 5-351)
`unexpected or failed Pluggable Transmission Module`	FACTERM	X	X[5]	X	X[6]	X	Procedure 5-143: "Clear "unexpected or failed Pluggable Transmission Module" alarm" (p. 5-353)
`Unknown Ring Type`	RNG-URT					X[2]	Procedure 5-144: "Clear "Unknown Ring Type" condition" (p. 5-356)
`unrecoverable hardware failure during download, replace CP`	FACTERM			X			Procedure 5-145: "Clear "unrecoverable hardware failure during download, replace CP" alarm" (p. 5-357)
`VCG Failure of LCAS Protocol (Sink)`	VCGFOPR	X	X	X	X[5,6]	X	Procedure 5-146: "Clear "VCG Failure of LCAS Protocol" alarms" (p. 5-359)

Table 2-1 Alcatel-Lucent 1665 DMX, Release 9.1 reported alarm list (continued)

Name	Probable Cause	ASAP[4]	Severity Level				Go to
			CR	MJ	MN	SC[1]	
`VCG Failure of LCAS Protocol (Source)`	VCGFOPT	X	X	X	X[5,6]	X	Procedure 5-146: "Clear "VCG Failure of LCAS Protocol" alarms" (p. 5-359)
`VCG Loss of Partial Capacity`	VCGLOPC	X	X	X	X[5,6]	X	Procedure 5-147: "Clear "VCG Loss of Partial Capacity" alarm" (p. 5-361)
`version mismatch`	FACTERM	X	X	X	X	X	Procedure 5-148: "Clear "version mismatch" alarm" (p. 5-365)
`waiting for download`	FACTERM					X[2]	No action is necessary.

Notes:

1. SC (Standing Conditions) are either events (usually user initiated such as switch requests) or alarms that are provisioned NA (Not Alarmed).
2. Standing conditions that are reported with an ABN condition in the alarm list. They are also identified on the SYSCTL faceplate by a lighted **ABN** LED.
3. STSN represent STS-1, STS-3c, STS-12c, STS-48c, and STS-192c.
4. The alarms/conditions with an X in the ASAP column indicate that the alarm/condition is part of an ASAP. The alarm/condition may be either an alarm or an event and is provisionable to CR, MJ, MN, NA (Not Alarmed), or NR (Not Reported). View the ASAP assigned to the specific entities to determine which alarm levels apply.
5. Service affecting default value.
6. Non-service affecting default value.
7. This alarm is provisionable to CR, MJ, or MN. This ASAP does not support NA (Not Alarmed) or NR (Not Reported).

3 Alarms, conditions, and error messages

Overview

Purpose

This chapter contains brief descriptions of the alarm messages for the Alcatel-Lucent 1665 Data Multiplexer.

Contents

−48V power/fuse FA failed

Description

The −48 volt power feeder "A" has either failed or been interrupted, or circuit breaker "A" on the shelf has tripped.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	System
AID Type	Fuse
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	PWR (Power failure)
Effect on Service	NSA
Alarm Entity Type	COM
Description	−48V power/fuse FA failed
Probable Cause	A −48 volt power feeder "A" has either failed or been interrupted, or circuit breaker "A" on the shelf has tripped.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-2: " Clear "−48V power/fuse FA or FB failed" alarm" (p. 5-13).

−48V power/fuse FB failed

Description

The −48 volt power feeder "B" has either failed or been interrupted, or circuit breaker "B" on the shelf has tripped.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	System
AID Type	Fuse
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	PWR (Power failure)
Effect on Service	NSA
Alarm Entity Type	COM
Description	−48V power/fuse FB failed
Probable Cause	A −48 volt power feeder "B" has either failed or been interrupted, or circuit breaker "B" on the shelf has tripped.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-2: “ Clear "−48V power/fuse FA or FB failed" alarm” (p. 5-13).

ABN condition

Description

A temporary condition exists that could potentially affect service (for example, a user-initiated protection switch or loopback).

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	System Control slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	MAN (Manually caused abnormal condition)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	ABN condition
Likely Cause	A temporary condition exists that could potentially affect service (for example, a user-initiated protection switch, lockout, or loopback).
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Locate the corresponding Not Alarmed (SC) in the alarm list, and proceed to the appropriate procedure to release/clear the condition.

ACO active

Description

Audible office alarms (normally active) are being suppressed.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	INHAUDB (Alarm audibles inhibited)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	ACO active
Likely Cause	User selected **Fault** → **Alarm Cutoff** or pressed the **ACO TEST** push button on SYSCTL circuit pack.
Visible Indication	Lighted **ACO** LED on the SYSCTL faceplate
Action	No action is necessary. The condition clears automatically when a new alarm is detected or all alarms clear.

AGNE communication failure

Description

The network element cannot establish communication with the designated alarm gateway network element (AGNE), or the AGNE cannot establish communication with a network element in the same alarm group, or the AGNE has lost communication with a network element in the same alarm group.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	System
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	PRCDRERR (Procedure error)
Effect on Service	NSA
Alarm Entity Type	COM
Description	AGNE communication failure
Likely Cause	Either the AGNE has not been provisioned or has failed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively).
Action	Proceed to Procedure 5-3: “Clear "AGNE communication failure" alarm” (p. 5-18).

AUTO link shutdown

Description

A remote client signal or VCG failure has been detected and the specified Data or Ethernet port has automatically shut down.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	Data Port Fast Ethernet Port Gigabit Ethernet Port
AID Type	Data port Ethernet port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	ALS (Auto Link Shutdown)
Effect on Service	SA
Alarm Entity Type	DATA FELAN GELAN
Description	AUTO link shutdown
Likely Cause	Either a remote client signal failure or a VCG failure has been detected and the port Remote Client Fail Link Shutdown parameter is enabled.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively).
Action	Proceed to Procedure 5-5: “Clear "AUTO link shutdown" alarm” (p. 5-24).

automatic lock

Description

A lockout of switching on a 1+1 equipment-protected pair (DS3/EC1, TMUX, or high-speed Main), because the provisioned threshold for number of switches has been exceeded.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	WKSWPR-1 (Working facility/equipment switched to protection unit 1) WKSWPR-2 (Working facility/equipment switched to protection unit 2)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	EQPT
Description	automatic lock
Likely Cause	System has locked protection switching between a 1+1 equipment-protected pair because the provisioned number of consecutive APS switches has occurred (DS3/EC1, TMUX, or high-speed Main).
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-6: “Clear "automatic lock" condition” (p. 5-26).

Automatic protection switch mode mismatch

Description

There is a mismatch detected in the APS channel, specifically K2 byte, bit 5 for the 1+1_BIDIR or 1+1_OPTM protection group. The APS channel is provided by the K1 and the K2 bytes in the SONET section overhead of an STS-N to communicate the protection switching protocol between the local and far-end nodes.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	1+1 Bidirectional Protection Group 1+1 Optimized Protection Group
AID Type	OC-N line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	APSMM (APS Mode Mismatch)
Effect on Service	NSA
Alarm Entity Type	OCN
Description	Automatic protection switch mode mismatch
Likely Cause	The OC-N line at the near-end network element has been provisioned to 1+1_BIDIR or 1+1_OPTM, but the OC-N line at the far-end network element has been provisioned to 1xN or 1+1 (unidirectional).
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-7: “Clear "Automatic protection switch mode mismatch" alarm” (p. 5-29).

Automatic protection switch primary section mismatch

Description

There is a mismatch detected in the primary section of the APS channel, specifically K2 byte, bits 1–4. Therefore, the near-end and far-end network elements of a 1+1_OPTM protection switching span do not agree on the primary section. The APS channel is provided by the K1 and the K2 bytes in the SONET section overhead of an STS-N to communicate the protection switching protocol between the local and far-end nodes.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	1+1 Optimized Protection Group
AID Type	OC-N line (1+1 optimized protection group)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	APSPSM (APS Primary Section Mismatch)
Effect on Service	NSA
Alarm Entity Type	OCN
Description	Automatic protection primary section mismatch
Likely Cause	User selected **Fault** → **Protection Switch** and highlighted 1+1_OPTM Line Protection Group, and provisioned the Switch Type as **Lockout**.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-8: “Clear "Automatic protection switch primary section mismatch" alarm” (p. 5-31).

Automatic protection switch unused codes

Description

The near-end network element received unexpected switching request codes in the APS channel (specifically, K1 byte, bits 1–4) in the protection switching request for a 1+1_OPTM protection group. The APS channel is provided by the K1 and the K2 bytes in the SONET section overhead of an STS-N to communicate the protection switching protocol between the local and far-end nodes.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	1+1 Optimized Protection Group
AID Type	OC-N line (1+1 optimized protection group)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	APSUC (APS unused codes)
Effect on Service	NSA
Alarm Entity Type	OCN
Description	Automatic protection unused codes
Likely Cause	The OC-N line at the near-end network element has been provisioned to 1+1_OPTM, but the OC-N line at the far-end network element has been provisioned to an incompatible protection group type.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-9: “Clear "Automatic protection switch unused codes" alarm” (p. 5-34).

Automatic protection switch unresolved transient codes

Description

The local node has attempted to communicate with far-end node of a 1+1_OPTM protection group and has not received the expected change in K-bytes from the far-end node. Transient codes are only received while the local node is waiting for a response from the far-end node or is in the process of responding to K-byte changes from the far-end node, yet they are persisting.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	1+1 Optimized Protection Group
AID Type	OC-N line (1+1 optimized protection group)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	APSUT (APS unresolved transient codes)
Effect on Service	NSA
Alarm Entity Type	OCN
Description	Automatic protection unresolved transient codes
Likely Cause	User selected **Fault** → **Protection Switch** and highlighted 1+1_OPTM Line Protection Group, and provisioned the Switch Type as **Lockout**. Or, the SYSCTL at the far-end network element is in the processing of resetting, therefore protection switching at the far-end is temporarily unavailable at the far end.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-10: “Clear "Automatic protection switch unresolved transient codes" alarm” (p. 5-36).

Circuit Provisioning Error

Description

Circuit has at least one provisioned source or destination (loca/locz) value that does not match the actual value.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	BLSR Protection Group
AID Type	STS-1, STS-3c, STS-12c, STS-48c, or STS-192c Ring Channel VT1.5 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	PAPRVERR (Path Provisioning Error)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Circuit Provisioning Error
Likely Cause	Circuit has an incorrectly provisioned source or destination.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-12: “Clear "Circuit Provisioning Error" alarm” (p. 5-43).

copy program IP

Description

The system is copying the software generic from the dormant area to a remote network element.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC (EOC failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	copy program IP
Likely Cause	User selected **Configuration** → **Software** → **Copy Software**.
Visible Indication	None
Action	No action is necessary. The condition clears automatically when the generic is copied to the dormant area of the destination network element.

CP contributing to a pack failure

Description

The specified circuit pack has contributed to the failure of another circuit pack.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	CTNEQPT (Facility/circuit interconnection equipment failure)
Effect on Service	NSA
Alarm Entity Type	EQPT
Description	CP contributing to a pack failure
Likely Cause	The circuit pack has contributed to the failure of another circuit pack.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the failed circuit pack.
Action	Proceed to Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44).

CP initialization IP

Description

The system is initializing the affected circuit pack.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	CP initialization IP
Likely Cause	A new circuit pack was installed in the slot and a reset was performed.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate. and a continuously lighted **Fault** LED on the affected circuit pack.
Action	No action is necessary. The condition clears automatically after the affected circuit pack initializes.

CP not allowed - crs

Description

The circuit pack does not support the cross-connection(s) currently provisioned for the slot.

Alarm Data	**Value/Meaning**
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	NSA
Alarm Entity Type	EQPT
Description	CP not allowed - crs
Likely Cause	A circuit pack was inserted into a slot that was already provisioned with cross-connections, and those provisioned cross-connections are not supported by the new circuit pack.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the affected circuit pack.
Action	Proceed to Procedure 5-14: “Clear "CP not allowed - crs" alarm” (p. 5-49).

CP not allowed - eqpt

Description

An unsupported circuit pack type is inserted into a slot.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	NSA
Alarm Entity Type	EQPT
Description	CP not allowed - eqpt
Likely Cause	A circuit pack was inserted into a slot that was already provisioned for another circuit pack type, and the new circuit pack is not supported by that slot. For example, an electrical circuit pack was inserted into slot G1/G2, and the circuit pack was not recognized by the SYSCTL.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the affected circuit pack.
Action	Proceed to Procedure 5-15: “Clear "CP not allowed - eqpt" alarm” (p. 5-51).

CP removed or CP failure

Description

A circuit pack was removed from the shelf, or the circuit pack has a failed power module.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	CP removed or CP failure
Likely Cause	An unprotected circuit pack carrying service was removed from the shelf, or the circuit pack power module failed: SA. A protected circuit pack or an unprotected circuit pack NOT carrying service was removed from the shelf, or the circuit pack power module failed: NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted Fault LED on a failed circuit pack.
Action	Proceed to Procedure 5-16: “Clear "CP removed or CP failure" alarm” (p. 5-53).

CP software upgrade required

Description

The firmware in the indicated circuit pack does not match the active software generic running on the network element.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	CP software upgrade required
Likely Cause	Either a new version of the software generic was applied to the shelf and the indicated circuit pack did not update automatically, or a new circuit pack was inserted into the shelf and the active software generic on the shelf does not match the new circuit pack.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-17: “Clear "CP software upgrade required" condition” (p. 5-55).

CPY-MEM backup IP

Description

Remote backup of provisioned data via file transfer protocol (FTP), FTAM-FTP gateway (FTTD), or FTAM is in progress.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC (EOC failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	CPY-MEM backup IP
Likely Cause	Either a user selected **Configuration** → **Software** → **Remote Backup** or a previously scheduled backup is now executing.
Visible Indication	None
Action	No action is necessary. The condition clears automatically when the backup is complete.

CPY-MEM download IP

Description

Download of a software generic via FTP, FTAM-FTP gateway (FTTD), or FTAM is in progress.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC (EOC failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	CPY-MEM download IP
Likely Cause	User selected **Configuration** → **Software** → **Download Software**.
Visible Indication	None
Action	No action is necessary. The condition clears automatically when the download is complete.

CPY-MEM restore IP

Description

Restoration of provisioned data from the backup file is in progress.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC (EOC failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	CPY-MEM restore IP
Likely Cause	User selected **Configuration** → **Software** → **Remote Restore**.
Visible Indication	None
Action	No action is necessary. The condition clears automatically when the restore is complete.

DATA CP failed

Description

Either an internal equipment failure of the specified Fibre Channel circuit pack was detected, or a communications problem between the Fibre Channel circuit pack and the System Controller (SYSCTL) circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA
Alarm Entity Type	EQPT
Description	DATA CP failed
Likely Cause	A Fibre Channel circuit pack carrying service failed. A failure on a Fibre Channel circuit pack is always SA as the Fibre Channel circuit packs are unprotected.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the failed circuit pack.
Action	Proceed to Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44).

DATA terminal loopback

Description

A loopback is active on the specified Data port.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Data port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	DATA
Description	DATA terminal loopback
Likely Cause	User selected **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-18: “Clear "DATA terminal loopback" condition” (p. 5-57).

Default K-bytes

Description

A bidirectional line-switched ring (BLSR) is detecting default K-bytes. When this alarm is present, protection switching at the BLSR node is unavailable.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	BLSR Protection Group
AID Type	OC-48 line OC-192 line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	BLSR-DKB (BLSR Default K-Bytes)
Effect on Service	NSA
Alarm Entity Type	OC48 OC192
Description	Default K-bytes
Likely Cause	A node is added or deleted from the BLSR; an adjacent node on the ring is being initialized; an adjacent node on the ring is being powered-up or powered-down; the provisioning of the nodes on the ring is inconsistent (for example, one or more nodes on the ring are provisioned to UPSR rather than BLSR).
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-19: “Clear "Default K-bytes" alarm” (p. 5-58).

dormant/exec code mismatch

Description

The software generic in the dormant area does not match the generic currently running on the network element.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC (EOC failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	dormant/exec code mismatch
Likely Cause	A software generic was downloaded (not applied) to the dormant area that is different than the software generic currently running on the network element.
Visible Indication	None
Action	Proceed to Procedure 5-20: “Clear "dormant/exec code mismatch" condition” (p. 5-61).

DS1 CP failed

Description

An internal equipment failure of the specified 28DS1/28DS1PM circuit pack was detected, or a communications problem between the specified circuit pack and the SYSCTL circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	DS1 CP failed
Likely Cause	An unprotected 28DS1 (LNW6) or 28DS1PM (LNW7) circuit pack failed - SA. A protected 28DS1 (LNW6) or 28DS1PM (LNW7) circuit pack failed - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the failed circuit pack.
Action	Proceed to Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44).

DS1E1 CP failed

Description

An internal equipment failure of the specified 56DS1/E1 circuit pack was detected, or a communications problem between the specified circuit pack and the SYSCTL circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	DS1E1 CP failed
Likely Cause	An unprotected 56DS1/E1 (LNW8) circuit pack failed - SA. A protected 56DS1/E1 circuit pack failed - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the failed circuit pack.
Action	Proceed to Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44).

DS1 loopback (to DSX)

Description

A loopback (toward the DSX) is active on the specified T1 port.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	DS1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	T1
Description	DS1 loopback (to DSX)
Likely Cause	User selected **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-21: “Clear "DS1 loopback (to DSX)" condition” (p. 5-62).

DS1 loopback (to Fiber)

Description

A loopback (toward the optical fiber) is active on the specified T1 port. Generally used during system start-up as a maintenance tool.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	DS1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	T1
Description	DS1 loopback (to Fiber)
Likely Cause	User selected **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-22: “Clear "DS1 loopback (to Fiber)" condition” (p. 5-63).

DS1 trmsn test IP

Description

A transmission test using the internal test signal generator and monitor is in progress on the specified T1 port.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	DS1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	T1
Description	DS1 trmsn test IP
Likely Cause	User selected **Fault** → **Test** → **Transmission**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	No action is necessary. Wait for the test to complete.

DS3 loopback (to DSX)

Description

A loopback (toward the DSX) is active on the specified T3 port.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	T3
Description	DS3 loopback (to DSX)
Likely Cause	User selected **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-23: “Clear "DS3 loopback (to DSX)" condition” (p. 5-64).

DS3 loopback (to Fiber)

Description

A loopback (toward the optical fiber) is active on the specified T3 port. Generally used during system start-up as a maintenance tool.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	T3
Description	DS3 loopback (to Fiber)
Likely Cause	User selected **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-24: “Clear "DS3 loopback (to Fiber)" condition” (p. 5-65).

DS3 trmsn test IP

Description

A transmission test using the internal test signal generator and monitor is in progress on the specified T3 port.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	T3
Description	DS3 trmsn test IP
Likely Cause	User selected **Fault** → **Test** → **Transmission**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	No action is necessary. Wait for the test to complete.

DS3EC1 CP failed

Description

An internal equipment failure of the specified 12DS3/EC1 or 48DS3/EC1 circuit pack (DS3 or EC-1 components) was detected, or a communications problem between the specified circuit pack and the SYSCTL circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	DS3EC1 CP failed
Likely Cause	An unprotected DS3/EC1 circuit pack failed - SA. A protected DS3/EC1 circuit pack failed - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the failed circuit pack.
Action	Proceed to Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44).

Duplicate Ring Node

Description

Two nodes in the BLSR have the same node identifier (NID) or the total number of nodes in the ring is more than 16.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	BLSR Protection Group
AID Type	BLSR protection group
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	DUPL-RNG (Duplicate Ring Node)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Duplicate Ring Node
Likely Cause	Two nodes on the BLSR have been provisioned with the same node identifier (NID) or a seventeenth ring node has been added to the ring.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-25: “Clear "Duplicate Ring Node" alarm” (p. 5-66).

E1 loopback (to DSX)

Description

A loopback (toward the DSX) is active on the specified E1 port.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	E1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	E1
Description	E1 loopback (to DSX)
Likely Cause	User selected **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-26: "Clear "E1 loopback (to DSX)" condition" (p. 5-68).

E1 loopback (to Fiber)

Description

A loopback (toward the optical fiber) is active on the specified E1 port. Generally used during system start-up as a maintenance tool.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	E1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	E1
Description	E1 loopback (to Fiber)
Likely Cause	User selected **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-27: “Clear "E1 loopback (to Fiber)" condition” (p. 5-69).

E1 trmsn test IP

Description

A transmission test using the internal test signal generator and monitor is in progress on the specified E1 port.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	E1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	E1
Description	E1 trmsn test IP
Likely Cause	User selected **Fault** → **Test** → **Transmission**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	No action is necessary. Wait for the test to complete.

EC1 loopback (to DSX)

Description

A loopback (toward the DSX) is active on the specified EC-1 port.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	EC-1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	EC1
Description	EC1 loopback (to DSX)
Likely Cause	User selected **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-28: “Clear "EC1 loopback (to DSX)" condition” (p. 5-70).

EC1 loopback (to Fiber)

Description

A loopback (toward the optical fiber) is active on the specified EC-1 port. Generally used during system start-up as a maintenance tool.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	EC-1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	EC1
Description	EC1 loopback (to Fiber)
Likely Cause	User selected **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-29: “Clear "EC1 loopback (to Fiber)" condition” (p. 5-71).

ECV - excessive code violation

Description

The Gigabit Ethernet circuit pack has received three consecutive invalid codes.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	Gigabit Ethernet port
AID Type	Gigabit Ethernet port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	ECV (Excessive Coding Violations - Ethernet)
Effect on Service	SA
Alarm Entity Type	GELAN
Description	ECV - excessive code violation
Likely Cause	A bad fiber connection, an intermittent failure of a Gigabit Ethernet circuit pack, or a problem on the fiber.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-30: “Clear "ECV - excessive code violation" alarm” (p. 5-72).

ENET facility loopback

Description

A facility loopback is active on the specified Ethernet LAN port.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Ethernet port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	ENET
Description	ENET facility loopback
Likely Cause	User selected **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-31: “Clear "ENET loopback" conditions” (p. 5-77).

ENET terminal loopback

Description

A terminal loopback is active on the specified Ethernet LAN port or Link Aggregation Group.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Ethernet port Link Aggregation Group
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	ENET
Description	ENET terminal loopback
Likely Cause	User selected **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-31: "Clear "ENET loopback" conditions" (p. 5-77).

ENNI signaling communication failure with peer

Description

The system cannot communicate with the far-end peer network element through the ENNI signaling communication channel.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	OCn Port
AID Type	OC-n Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SIGPEER (ENNI signaling communication failure with peer)
Effect on Service	NSA
Alarm Entity Type	COM
Description	ENNI signaling communication failure with peer
Likely Cause	A SONET or DCC-related failure has occurred. A LAN-3 failure has occurred. A manual IP route provisioning error occurred. SYSCTL circuit pack failed, reset, or initialized at the far-end peer network element. The program installation failed at the far-end network element. The program installation is in progress at the far-end network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-32: “Clear "ENNI signaling communication failure with peer" alarm” (p. 5-78).

environmentn

Description

The specified environmental alarm point (miscellaneous discrete input) is active. The actual message that appears in the alarm and status report for this condition can be provisioned; environment is the default message. It is provisioned by selecting **Configuration** → **Misc. Discretes**.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA) Default: Minor (MN)
AID Type	Environmental Alarm Input
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	MISC (Miscellaneous condition)
Effect on Service	CR, MJ, MN = NSA Not Alarmed = Standing Condition (SC)
Alarm Entity Type	ENV (CR, MJ, MN) COM (SC)
Description	environment1 . . . environment14 environment15 is used for fan failure; it cannot be provisioned. environment16 . . . environment19 (or provisioned message)
Likely Cause	Some external equipment has operated a contact closure connected to that input.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively). None when the severity level is provisioned to NA.
Action	Proceed to Procedure 5-33: "Clear "environmentn" alarm" (p. 5-82).

Equipment configuration no longer supported

Description

The system has detected a circuit pack configuration that is not supported by the current software release.

Alarm Data	Value/Meaning
Severity Levels	Minor (MN)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	DATAFLT (Data Integrity Fault)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Equipment configuration no longer supported
Likely Cause	A function/growth group is equipped with an LNW66/71 circuit pack in one slot and an LNW70/78 circuit pack in the companion slot. This circuit pack combination is not supported in this release.
Visible Indication	Lighted **MN** LED on the SYSCTL faceplate
Action	Proceed to Procedure 5-44: “Clear "Generic/Database/Equipment Configuration" alarms/conditions” (p. 5-104).

ERP - Multiple RPL Owners

Description

The node provisioned as the RPL Owner received messages that it did not originate that should only come from an RPL Owner.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	Fast Ethernet port Gigabit Ethernet port VCG port
AID Type	Ethernet 10/100T port Ethernet GbE port VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	ERP-MO (ERP - Multiple RPL Owners)
Effect on Service	SA
Alarm Entity Type	FELAN GELAN VCG
Description	ERP - Multiple RPL Owners
Likely Cause	More than one node in the ring is provisioned as the RPL owner.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively).
Action	Proceed to Procedure 5-34: “Clear "ERP - Multiple RPL Owners" alarm” (p. 5-83).

ERP - PDU Watchdog Timeout

Description

A non-RPL owner node hasn't received R-APS PDUs for 1 minute on both ports (both links are good) or the ring is in the protection state due to a non-local failure (meaning some other node should be sending PDUs), and the RPL-owner node hasn't received R-APS PDUs for 1 minute on both ports.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	Fast Ethernet port Gigabit Ethernet port VCG port
AID Type	Ethernet 10/100T port Ethernet GbE port VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	ERP-WD (ERP - PDU Watchdog Timeout)
Effect on Service	SA
Alarm Entity Type	FELAN GELAN VCG
Description	ERP - PDU Watchdog Timeout
Likely Cause	No RPL Owner is provisioned (or it is shut down), or this node might be using the wrong VLAN or MD level or the R-APS virtual channel may be down.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively).
Action	Proceed to Procedure 5-35: "Clear "ERP - PDU Watchdog Timeout" alarm" (p. 5-85).

Exceeded MTU size drop

Description

The specified port has detected the Exceeded MTU size drop ratio (Exceeded MTU size drop count/Total frame received count) surpassed the provisioned Exceeded MTU size drop threshold.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	Fast Ethernet port Gigabit Ethernet port VCG port
AID Type	Ethernet 10/100T port Ethernet GbE port VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EMSD (Exceeded MTU Size Drop)
Effect on Service	NSA
Alarm Entity Type	FELAN GELAN VCG
Description	Exceeded MTU size drop
Likely Cause	Local port/VCG provisioning error, or a provisioning error or equipment failure in the network.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively).
Action	Proceed to Procedure 5-36: “Clear "Exceeded MTU size drop" alarm” (p. 5-88).

excessive holdover

Description

The system has been in holdover mode for more than 24 hours. This may cause degraded performance (high error rates) on the transmitted and/or received signals. When this condition exists, the system also reports the `holdover mode active` condition.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	System
AID Type	Shelf Subshelf
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LHI (Loss of holdover integrity)
Effect on Service	NSA
Alarm Entity Type	COM
Description	excessive holdover
Likely Cause	The system was manually switched to holdover mode (by selecting **Fault** → **Timing/Sync Protection Switch** → **Clock Mode Switch**) and the switch has not been reset. The system is provisioned for sync message signaling, but the upstream system from which it line-times has not been provisioned for sync message signaling. The system automatically switched to holdover mode due to failure of the timing references and: • The reference failures have not cleared. • The system is provisioned for nonrevertive synchronization mode. • The system is provisioned for External timing and no external timing references are available. • The system is provisioned for line-timed operation and the optical line or OLIU circuit pack has failed, or a message indicating an upstream clock problem has been received on the sync message bits of the optical line.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-45: "Clear "holdover" conditions/alarms" (p. 5-113).

Excessive Reserved Rate on RPR

Description

The sum of all the provisioned VCG RPR span *Reserved Class A Add Rates* (Mb/s) around the ring has exceeded the link rate of the ring. The link rate is approximately 48.384 Mb/s per STS-1 cross-connection to the VCG.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EXS-RSV (RPR - Excessive Reserved Rate)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	VCG
Description	Excessive Reserved Rate on RPR
Likely Cause	The sum of all provisioned Class A reservations around the ring has exceeded the link rate of the ring.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-37: “Clear "Excessive Reserved Rate on RPR" condition” (p. 5-90).

Extra Traffic Preempted

Description

The protection channels in a high-speed OC-48 or OC-192 2-fiber BLSR were provisioned to carry additional working traffic and a failure or external switch request resulted in that extra traffic being preempted for service.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OC-48 line OC-192 line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RNG-PREEMPT (BLSR Extra Traffic Pre-empted)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	OC48 OC192
Description	Extra Traffic Preempted
Likely Cause	A failure was detected at some point on the BLSR, and the resulting protection switch preempted the extra traffic provisioned on the protection channels.
Visible Indication	None
Action	Proceed to Procedure 5-38: “Clear "Extra Traffic Preempted" condition” (p. 5-93).

fan shelf failed

Description

The fan shelf failed or the fan filter is clogged.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), or Not Alarmed (NA) Default: Major (MJ)
AID Type	System Control slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EXT (External failure)
Effect on Service	CR, MJ, MN = NSA Not Alarmed = Standing Condition (SC)
Alarm Entity Type	EQPT
Description	fan shelf failed
Likely Cause	The fan shelf failed or the fan filter is clogged.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively). None when the severity level is provisioned to NA.
Action	Proceed to Procedure 5-39: “Clear "fan shelf failed" alarm” (p. 5-95).

far end not LCAS

Description

Link capacity adjustment scheme (LCAS) is enabled at the near end, but the far end does not support LCAS.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	NOTLCAS (Far End Not LCAS)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	VCG
Description	far end not LCAS
Likely Cause	At the near end, LCAS is enabled on the designated VCG. At the far end, LCAS is either not enabled or not supported.
Visible Indication	None
Action	Proceed to Procedure 5-40: "Clear "far end not LCAS" condition" (p. 5-99)

Far-end protection line failure

Description

In a bidirectional 1+1 system, the near-end terminal received K1 bytes indicating that the far-end terminal is no longer receiving the near-end requests or the far-end terminal considers the near-end requests invalid.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	1+1 Bidirectional Protection Group
AID Type	OC-N line (1+1 bidirectional protection group)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FEPRLF (Far-end Protection Line Failure)
Effect on Service	NSA
Alarm Entity Type	OCN
Description	Far-end protection line failure
Likely Cause	Alarm condition was detected at the far-end OC-N OLIU.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-41: "Clear "Far-end protection line failure" alarm" (p. 5-101).

FE-LAN CP failed

Description

An internal equipment failure of the specified 10/100 Fast Ethernet circuit pack was detected, or a communications problem between the 10/100 Fast Ethernet pack and the SYSCTL circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA
Alarm Entity Type	EQPT
Description	FE-LAN CP failed
Likely Cause	A 10/100 Fast Ethernet circuit pack failed. A failure on a 10/100 Fast Ethernet circuit pack is always SA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the failed circuit pack.
Action	Proceed to Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44).

forced switch

Description

A user-initiated forced protection switch is active on a 1+1 OC-N line, 1+1_BIDIR OC-N line, 1+1_OPTM OC-N line, a path switched ring, or a 1+1 equipment-protected pair.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OC-3, OC-12, OC-48, OC-192 line STS-1, STS-3c, STS-12c, STS-48c, or STS-192c Ring Channel VT1.5 Ring Channel Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	WKSWPR-1 (Working facility/equipment switched to protection unit 1) WKSWPR-2 (Working facility/equipment switched to protection unit 2)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	OC3, OC12, OC48, OC192 STS1, STS3C, STS12C, STS48C, or STS192C VT1 Slot = EQPT
Description	forced switch
Likely Cause	User selected **Fault** → **Protection Switch**, highlighted a 1+1 Equip, 1+1 Line, 1+1_BIDIR line, 1+1_OPTM Line, or Path Protection Group, and provisioned the Switch Type as **Forced**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-42: “Clear "forced switch" condition” (p. 5-102).

Forced Switch

Description

The protection tributaries (in the specified direction [East or West] on the 2-fiber BLSR) are selected unless there is an existing lockout or forced protection switching request.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OC-48 line OC-192 line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FSR (Forced Switch)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	OC48 OC192
Description	Forced Switch
Likely Cause	User executed a manual switch on the 2-fiber BLSR using **Fault** → **Protection Switch** and selected Force To Protection, Ring.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-43: “Clear "Forced Switch" condition” (p. 5-103).

GE-LAN CP failed

Description

An internal equipment failure of the specified Gigabit Ethernet circuit pack was detected, or a communication problem between the Gigabit Ethernet circuit pack and the SYSCTL circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA
Alarm Entity Type	EQPT
Description	GE-LAN CP failed
Likely Cause	A Gigabit Ethernet circuit pack failed. A failure on a Gigabit Ethernet circuit pack is always SA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the failed circuit pack.
Action	Proceed to Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44).

generic validation IP

Description

The system is validating the generics stored in nonvolatile memory (NVM).

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC (EOC failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	generic validation IP
Likely Cause	The system is validating the generics stored in NVM.
Visible Indication	None
Action	No action is necessary. The condition clears automatically after all generics in NVM are validated.

holdover mode active

Description

The system is in holdover synchronization mode.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Shelf Subshelf
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	HOLDOVRSYNC (Holdover synchronization mode)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	holdover mode active
Likely Cause	The system was manually switched to holdover mode (by selecting **Fault** → **Timing/Sync Protection Switch** → **Clock Mode Switch**) and the switch has not been reset. The system is provisioned for sync message signaling, but the upstream system from which it line-times has not been provisioned for sync message signaling. The system automatically switched to holdover mode due to failure of the timing references and: • The reference failures have not cleared. • The system is provisioned for nonrevertive synchronization mode. • The system is provisioned for External timing and no external timing references are available. • The system is turned-up with default conditions and no incoming external timing input signal is present. • The system is provisioned for line-timed operation and the optical line or OLIU circuit pack has failed, or a message indicating an upstream clock problem has been received on the sync message bits of the optical line.
Visible Indication	None
Action	Proceed to Procedure 5-45: “Clear "holdover" conditions/alarms” (p. 5-113).

illegal CP type

Description

A circuit pack is present in a slot in a shelf configuration not supported by the software to provide transmission.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	illegal CP type
Likely Cause	A slot was occupied and provisioned for a supported circuit pack type. The supported circuit pack was removed, and an unsupported circuit pack type was inserted into that slot: SA. An illegal or unknown circuit pack type has been inserted into the shelf: NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-46: “Clear "illegal CP type" alarm” (p. 5-115).

Improper APS Codes

Description

Received automatic protection switch (APS) codes are not appropriate for the current bidirectional line-switched ring (BLSR) switch state. Therefore, the switch request on the BLSR does not complete properly.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	BLSR Protection Group
AID Type	OC-48 line OC-192 line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	APSPROV (Improper APS Codes)
Effect on Service	NSA
Alarm Entity Type	OC48 OC192
Description	Improper APS Codes
Likely Cause	A node in the BLSR is isolated due to • An OC-48/OC-192 OLIU circuit pack failure • A SYSCTL circuit pack failure, reset, or initialization • An inc. OC-48/OC-192 sig. degrade or inc. OC-48/OC-192 sig. failed alarm at some point on the BLSR.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-47: "Clear "Improper APS Codes" alarm" (p. 5-117).

inc. data type mismatch

Description

The alarm indicates that the Payload Type Identifier in the GFP header does not match the expected value client type (Ethernet or Fibre Channel [FC]). The alarm is valid on the LNW63, LNW66, LNW67, LNW68, and LNW73/73C circuit packs.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	MISC (Miscellaneous condition)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	VCG
Description	inc. data type mismatch
Likely Cause	Inconsistent Equipage: One end of a circuit is equipped with an Ethernet pack and the other end is equipped with a Fiber Channel pack. Incorrect cross-connect provisioning: An Ethernet pack is connected through the network to a Fiber Channel pack. Inconsistent GFP FCS provisioning.
Visible Indication	None
Action	Proceed to Procedure 5-48: “Clear "inc. data type mismatch" alarm” (p. 5-121).

inc. DS1 sync. ref. AIS

Description

DS1 alarm indication signal (AIS) is being received from the DS1 synchronization reference signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Unprotected default: Major (MJ) Protected default: Minor (MN)
ASAP Type	System Timing
AID Type	Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Loss of timing on both primary and secondary synchronization references) SYNC (Loss of timing on a protected synchronization reference)
Effect on Service	NSA
Alarm Entity Type	T1
Description	inc. DS1 sync. ref. AIS
Likely Cause	Failure of the timing supply that provides the DS1 timing reference.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-49: “Clear "inc. DS1/E1 sync. ref." alarms” (p. 5-125).

inc. DS1 sync. ref. BER

Description

The bit error ratio (BER) in the DS1 synchronization reference signal exceeds 10^{-3}.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Unprotected default: Major (MJ) Protected default: Minor (MN)
ASAP Type	System Timing
AID Type	Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Loss of timing on both primary and secondary synchronization references) SYNC (Loss of timing on a protected synchronization reference)
Effect on Service	NSA
Alarm Entity Type	T1
Description	inc. DS1 sync. ref. BER
Likely Cause	Failure of the timing supply that provides the DS1 timing reference. See DS1 sync. ref LOS.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-49: “Clear "inc. DS1/E1 sync. ref." alarms” (p. 5-125).

inc. DS1 sync. ref. EOOF

Description

Excessive out-of-frame (EOOF) events were detected in the DS1 synchronization reference signal. An EOOF is defined as more than 512 out-of-frame events in one day.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Unprotected default: Major (MJ) Protected default: Minor (MN)
ASAP Type	System Timing
AID Type	Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Loss of timing on both primary and secondary synchronization references) SYNC (Loss of timing on a protected synchronization reference)
Effect on Service	NSA
Alarm Entity Type	T1
Description	inc. DS1 sync. ref. EOOF
Likely Cause	Failure of the timing supply that provides the DS1 timing reference.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-49: “Clear "inc. DS1/E1 sync. ref." alarms” (p. 5-125).

inc. DS1 sync. ref. LOF

Description

The system has detected a DS1 loss-of-frame (LOF) condition for the incoming DS1 synchronization reference signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Unprotected default: Major (MJ) Protected default: Minor (MN)
ASAP Type	System Timing
AID Type	Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Loss of timing on both primary and secondary synchronization references) SYNC (Loss of timing on a protected synchronization reference)
Effect on Service	NSA
Alarm Entity Type	T1
Description	inc. DS1 sync. ref. LOF
Likely Cause	Failure of the timing supply that provides the DS1 timing reference.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-49: “Clear "inc. DS1/E1 sync. ref." alarms” (p. 5-125).

inc. DS1 sync. ref. LOS

Description

The system has detected a DS1 loss-of-signal (LOS) condition for the incoming DS1 synchronization reference signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Unprotected default: Major (MJ) Protected default: Minor (MN)
ASAP Type	System Timing
AID Type	Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Loss of timing on both primary and secondary synchronization references) SYNC (Loss of timing on a protected synchronization reference)
Effect on Service	NSA
Alarm Entity Type	T1
Description	inc. DS1 sync. ref. LOS
Likely Cause	Failure of the timing supply that provides the DS1 timing reference. The system is turned-up with default conditions and no incoming external timing input signal is present.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-49: “Clear "inc. DS1/E1 sync. ref." alarms” (p. 5-125).

inc. DS1 sync. ref. OOL

Description

The incoming DS1 synchronization reference signal is out of lock (OOL). The frequency of the clock providing the DS1 reference signal is out of specification.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Unprotected default: Major (MJ) Protected default: Minor (MN)
ASAP Type	System Timing
AID Type	Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Loss of timing on both primary and secondary synchronization references) SYNC (Loss of timing on a protected synchronization reference)
Effect on Service	NSA
Alarm Entity Type	T1
Description	inc. DS1 sync. ref. OOL
Likely Cause	Failure of the timing supply that provides the DS1 timing reference.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-49: “Clear "inc. DS1/E1 sync. ref." alarms” (p. 5-125).

inc. DS3 Cbit Mismatch

Description

Indicates a difference between the framing of the incoming DS3 signal (from the DSX) and the provisioned framing mode of the receiving port.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	DS3 Port
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	CBITMM (C-Bit Mismatch)
Effect on Service	SA or NSA
Alarm Entity Type	T3
Description	inc. DS3 Cbit Mismatch
Likely Cause	The incoming DS3 signal is provisioned for the M13 frame format and the local DS3 port is provisioned for the CBIT frame format.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-52: “Clear "inc. DS3 Cbit Mismatch" alarm” (p. 5-134).

inc. E1 sync. ref. AIS

Description

E1 alarm indication signal (AIS) is being received from the E1 synchronization reference signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Unprotected default: Major (MJ) Protected default: Minor (MN)
ASAP Type	System Timing
AID Type	Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Loss of timing on both primary and secondary synchronization references) SYNC (Loss of timing on a protected synchronization reference)
Effect on Service	NSA
Alarm Entity Type	E1
Description	inc. E1 sync. ref. AIS
Likely Cause	Failure of the timing supply that provides the E1 timing reference.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-49: “Clear "inc. DS1/E1 sync. ref." alarms” (p. 5-125).

inc. E1 sync. ref. BER

Description

The bit error ratio (BER) in the E1 synchronization reference signal exceeds 10^{-3}.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Unprotected default: Major (MJ) Protected default: Minor (MN)
ASAP Type	System Timing
AID Type	Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Loss of timing on both primary and secondary synchronization references) SYNC (Loss of timing on a protected synchronization reference)
Effect on Service	NSA
Alarm Entity Type	E1
Description	inc. E1 sync. ref. BER
Likely Cause	Failure of the timing supply that provides the E1 timing reference. See inc. E1 sync. ref LOS.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-49: “Clear "inc. DS1/E1 sync. ref." alarms” (p. 5-125).

inc. E1 sync. ref. CRC-4 MFA mismatch

Description

Indicates a difference between the signal format of the incoming E1 synchronization reference signal and the provisioned signal format of the receiving E1 timing input port.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	System Timing
AID Type	Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Loss of timing on both primary and secondary synchronization references) SYNC (Loss of timing on a protected synchronization reference)
Effect on Service	NSA
Alarm Entity Type	E1
Description	inc. E1 sync. ref. CRC-4 MFA mismatch
Likely Cause	The E1 timing input port is provisioned to receive a CRC-4 formatted E1 synchronization reference signal and the incoming E1 synchronization reference signal is a non-CRC-4 formatted E1 signal.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-49: “Clear "inc. DS1/E1 sync. ref." alarms” (p. 5-125).

inc. E1 sync. ref. LOF

Description

The system has detected a E1 loss-of-frame (LOF) condition for the incoming E1 synchronization reference signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Unprotected default: Major (MJ) Protected default: Minor (MN)
ASAP Type	System Timing
AID Type	Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Loss of timing on both primary and secondary synchronization references) SYNC (Loss of timing on a protected synchronization reference)
Effect on Service	NSA
Alarm Entity Type	E1
Description	inc. E1 sync. ref. LOF
Likely Cause	Failure of the timing supply that provides the E1 timing reference.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-49: "Clear "inc. DS1/E1 sync. ref." alarms" (p. 5-125).

inc. E1 sync. ref. LOS

Description

The system has detected a E1 loss-of-signal (LOS) condition for the incoming E1 synchronization reference signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Unprotected default: Major (MJ) Protected default: Minor (MN)
ASAP Type	System Timing
AID Type	Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Loss of timing on both primary and secondary synchronization references) SYNC (Loss of timing on a protected synchronization reference)
Effect on Service	NSA
Alarm Entity Type	E1
Description	inc. E1 sync. ref. LOS
Likely Cause	Failure of the timing supply that provides the E1 timing reference.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-49: “Clear "inc. DS1/E1 sync. ref." alarms” (p. 5-125).

inc. E1 sync. ref. OOL

Description

The incoming E1 synchronization reference signal is out of lock (OOL). The frequency of the clock providing the E1 reference signal is out of specification.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Unprotected default: Major (MJ) Protected default: Minor (MN)
ASAP Type	System Timing
AID Type	Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Loss of timing on both primary and secondary synchronization references) SYNC (Loss of timing on a protected synchronization reference)
Effect on Service	NSA
Alarm Entity Type	E1
Description	inc. E1 sync. ref. OOL
Likely Cause	Failure of the timing supply that provides the E1 timing reference.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-49: “Clear "inc. DS1/E1 sync. ref." alarms” (p. 5-125).

inc. (from DSX) DS1 AIS

Description

DS1 alarm indication signal (AIS) is being received from the near-end DS1 termination.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS1 Port
AID Type	DS1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	AIS (AIS Detected)
Effect on Service	SA or NSA
Alarm Entity Type	T1
Description	inc. (from DSX) DS1 AIS
Likely Cause	The upstream equipment failed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-50: "Clear "inc. (from DSX) DS1" alarms" (p. 5-128).

inc. (from DSX) DS1 LOF

Description

The system has detected a loss-of-frame (LOF) condition in an incoming DS1 signal. LOF is declared when an out-of-frame (OOF) defect persists for 2.5 (±0.5) seconds, except when AIS is present.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS1 Port
AID Type	DS1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOF (Loss of frame)
Effect on Service	SA or NSA
Alarm Entity Type	T1
Description	inc. (from DSX) DS1 LOF
Likely Cause	The upstream DS1 terminal equipment failed or there is incorrect DS1 port provisioning at either the upstream DS1 terminal equipment or the local network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-50: "Clear "inc. (from DSX) DS1" alarms" (p. 5-128).

inc. (from DSX) DS1 LOS

Description

At least 128 consecutive zeros are received in the DS1 signal incoming from the DSX-1, or the energy at the DS1 input is below a preset threshold.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS1 Port
AID Type	DS1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOS (Loss of Signal)
Effect on Service	SA or NSA
Alarm Entity Type	T1
Description	inc. (from DSX) DS1 LOS
Likely Cause	Hard failure of upstream equipment or facility (towards DSX-1). The DS1 input was disconnected at either the backplane or the DSX-1. Equipment is failed or removed at DSX-1.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-50: “Clear "inc. (from DSX) DS1" alarms” (p. 5-128).

inc. (from DSX) DS1 RAI

Description

The system has detected an incoming Remote Alarm Indication (RAI) at the specified local DS1 port.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS1 Port
AID Type	DS1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RAI (Remote alarm indication)
Effect on Service	NSA
Alarm Entity Type	T1
Description	inc. (from DSX) DS1 RAI
Likely Cause	A remote incoming signal failure was detected at the interfacing customer equipment that terminates the DS1.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-53: “Clear "inc. (from DSX) DSn RAI" alarm” (p. 5-137).

inc. (from DSX) DS1 sig. failed

Description

The bit error ratio (BER) in the DS1 signal incoming from the DSX-1 exceeds the provisioned failure threshold of 10^{-3} (default).

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS1 Port
AID Type	DS1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	T-BERL (incoming line signal BER thresholds exceeded)
Effect on Service	SA or NSA
Alarm Entity Type	T1
Description	inc. (from DSX) DS1 sig. failed
Likely Cause	Mismatch of line code (AMI/B8ZS) Failure of upstream equipment or facility (towards the DSX-1) Cross-talk in office wiring Failure of the 28DS1/28DS1PM or 56DS1/E1 circuit pack.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-50: “Clear "inc. (from DSX) DS1" alarms” (p. 5-128).

inc. (from DSX) DS3 AIS

Description

DS3 alarm indication signal (AIS) is being received from the far-end DS3 termination.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	DS3 Port
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	AIS (AIS detected)
Effect on Service	SA or NSA
Alarm Entity Type	T3
Description	inc. (from DSX) DS3 AIS
Likely Cause	The upstream equipment failed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-51: "Clear "inc. (from DSX) DS3" alarms" (p. 5-131).

inc. (from DSX) DS3 IDLE

Description

A DS3 IDLE signal is being received from the near-end DSX-3. The system reports this condition when an incoming DS3 IDLE signal persists for 2.5 (±0.5) seconds.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	DS3 Port
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	IDLE (Idle condition detected)
Effect on Service	SA or NSA
Alarm Entity Type	T3
Description	inc. (from DSX) DS3 IDLE
Likely Cause	The upstream equipment either failed or lower rate (DS2 or DS1) equipment was removed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-51: “Clear "inc. (from DSX) DS3" alarms” (p. 5-131).

inc. (from DSX) DS3 LOF

Description

The system has detected a loss-of-frame (LOF) condition in an incoming DS3 signal. LOF is declared when an out-of-frame (OOF) defect persists for 2.5 (±0.5) seconds.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	DS3 Port
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOF (Loss of frame)
Effect on Service	SA or NSA
Alarm Entity Type	T3
Description	inc. (from DSX) DS3 LOF
Likely Cause	The upstream DS3 terminal equipment failed or there is incorrect DS3 port provisioning at either the upstream DS3 terminal equipment or the local network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-51: “Clear "inc. (from DSX) DS3" alarms” (p. 5-131).

inc. (from DSX) DS3 LOS

Description

At least 128 consecutive zeros are received in the DS3 signal incoming from the DSX-3, or the energy at the DS3 input is below a preset threshold.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	DS3 Port
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOS (Loss of signal)
Effect on Service	SA or NSA
Alarm Entity Type	T3
Description	inc. (from DSX) DS3 LOS
Likely Cause	Hard failure of upstream terminal equipment or facility (towards the DSX-3), The DS3 input was disconnected at either the backplane or DSX-3, or The DSX-3 equipment is failed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-51: “Clear "inc. (from DSX) DS3" alarms” (p. 5-131).

inc. (from DSX) DS3 RAI

Description

The system has detected an incoming Remote Alarm Indication (RAI) at the specified local DS3 port.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS3 Port
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RAI (Remote alarm indication)
Effect on Service	NSA
Alarm Entity Type	T3
Description	inc. (from DSX) DS3 RAI
Likely Cause	A remote incoming signal failure was detected at the interfacing customer equipment that terminates the DS3 path.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-53: “Clear "inc. (from DSX) DSn RAI" alarm” (p. 5-137).

inc. (from DSX) DS3 sig. failed

Description

The bit error ratio (BER) in the DS3 signal incoming from the DSX-3 exceeds the provisioned failure threshold of 10^{-6} (default).

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	DS3 Port
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	T-BERL (incoming line signal BER thresholds exceeded)
Effect on Service	SA or NSA
Alarm Entity Type	T3
Description	inc. (from DSX) DS3 sig. failed
Likely Cause	Failure of the upstream equipment or facility (towards the DSX-3) Cross talk in office wiring Failure of DS3 circuit pack (12DS3/EC1, 48DS3/EC1, or TMUX).
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-51: “Clear "inc. (from DSX) DS3" alarms” (p. 5-131).

inc. (from fiber) DS1 AIS

Description

An LNW20 TMUX port in the portless mode is receiving a DS1 alarm indication signal (AIS) from the far-end DS1 termination.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS1 Port
AID Type	DS1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	AIS-EGR (AIS Detected in Egress direction)
Effect on Service	NSA
Alarm Entity Type	T1
Description	inc. (from fiber) DS1 AIS
Likely Cause	A problem/failure occurred at either the far-end SONET network element or the interfacing customer equipment connected to the far-end SONET network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-54: “Clear "inc. (from fiber) DSn" alarms” (p. 5-139).

inc. (from fiber) DS1 LOF

Description

An LNW20 TMUX port in the portless mode has detected a loss-of-frame (LOF) condition from the fiber. LOF is declared when an out-of-frame (OOF) defect persists for 2.5 (±0.5) seconds.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS1 Port
AID Type	DS1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOF-EGR (Loss of Frame in Egress direction)
Effect on Service	NSA
Alarm Entity Type	T1
Description	inc. (from fiber) DS1 LOF
Likely Cause	The local DS1 port is incorrectly provisioned, or a problem/failure occurred at either the far-end SONET network element or the interfacing customer equipment connected to the far-end SONET network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-54: “Clear "inc. (from fiber) DSn" alarms” (p. 5-139).

inc. (from fiber) DS1 RAI

Description

An LNW20 TMUX port in the portless mode has detected an incoming Remote Alarm Indication (RAI).

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS1 Port
AID Type	DS1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RAI-EGR (Remote Alarm Indication in Egress Position)
Effect on Service	NSA
Alarm Entity Type	T1
Description	inc. (from fiber) DS1 RAI
Likely Cause	A remote incoming signal failure was detected at the interfacing customer equipment that is connected to the far-end SONET network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-55: “Clear "inc. (from fiber) DSn RAI" alarms” (p. 5-141).

inc. (from fiber) DS3 AIS

Description

DS3 alarm indication signal (AIS) is being received from the far-end DS3 termination.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS3 Port
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	AIS-EGR (AIS Detected in Egress direction)
Effect on Service	NSA
Alarm Entity Type	T3
Description	inc. (from fiber) DS3 AIS
Likely Cause	A problem/failure occurred at either the far-end SONET network element or the interfacing customer equipment connected to the far-end SONET network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-54: “Clear "inc. (from fiber) DSn" alarms” (p. 5-139).

inc. (from fiber) DS3 LOF

Description

The system has detected a loss-of-frame (LOF) condition from the fiber. LOF is declared when an out-of-frame (OOF) defect persists for 2.5 (±0.5) seconds. This alarm was previously called inc. (from fiber) DS3 OOF.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS3 Port
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOF-EGR (Loss of Frame in Egress direction
Effect on Service	NSA
Alarm Entity Type	T3
Description	inc. (from fiber) DS3 LOF
Likely Cause	The local DS3 port is incorrectly provisioned, or a problem/failure occurred at either the far-end SONET network element or the interfacing customer equipment connected to the far-end SONET network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-54: "Clear "inc. (from fiber) DSn" alarms" (p. 5-139).

inc. (from fiber) DS3 RAI

Description

The system has detected an incoming Remote Alarm Indication (RAI) at the specific port. For C-bit, the RAI is declared when the far end detects a service-affecting equipment failure, DS3 LOS, DS3 LOF, or DS3 AIS. For M13, the RAI is declared when the far end detects a DS3 severely errored frame.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS3 Port
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RAI-EGR (Remote Alarm Indication in Egress Position)
Effect on Service	NSA
Alarm Entity Type	T3
Description	inc. (from fiber) DS3 RAI
Likely Cause	A remote incoming signal failure was detected at the interfacing customer equipment that is connected to the far-end SONET network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-55: “Clear "inc. (from fiber) DSn RAI" alarms” (p. 5-141).

inc. (from DSX) E1 AIS

Description

E1 alarm indication signal (AIS) is being received from the near-end E1 termination. Alcatel-Lucent 1665 DMX sends AIS downstream.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	E1 Port
AID Type	E1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	AIS (AIS detected)
Effect on Service	SA or NSA
Alarm Entity Type	E1
Description	inc. (from DSX) E1 AIS
Likely Cause	The upstream equipment failed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-56: "Clear "inc. (from DSX) E1" alarms" (p. 5-142).

inc. (from DSX) E1 LOF

Description

The system has detected a loss-of-frame (LOF) condition in an incoming E1 signal. Basic frame alignment is lost when either three consecutive incorrect frame alignment signals are detected or three consecutive non frame alignment signals are detected.
Alcatel-Lucent 1665 DMX sends AIS downstream.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	E1 Port
AID Type	E1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOF (Loss of frame)
Effect on Service	SA or NSA
Alarm Entity Type	E1
Description	inc. (from DSX) E1 LOF
Likely Cause	The upstream E1 terminal equipment failed or there is incorrect E1 port provisioning at either the upstream E1 terminal equipment or the local network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-56: “Clear "inc. (from DSX) E1" alarms” (p. 5-142).

inc. (from DSX) E1 LOS

Description

Loss of signal is detected when the incoming E1 signal level is less than or equal to 35 dB below normal for N consecutive pulse intervals (N is greater than 10 and less than 255). Alcatel-Lucent 1665 DMX sends AIS downstream.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	E1 Port
AID Type	E1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOS (Loss of signal)
Effect on Service	SA or NSA
Alarm Entity Type	E1
Description	inc. (from DSX) E1 LOS
Likely Cause	Hard failure of upstream equipment or facility (towards DSX-1) The E1 input was disconnected at either the backplane or the DSX-1 Equipment is failed or removed at DSX-1.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-56: "Clear "inc. (from DSX) E1" alarms" (p. 5-142).

inc. (from DSX) E1 sig. failed

Description

The bit error ratio (BER) based on bipolar violations in the E1 signal incoming from the DSX-1 exceeds the provisioned threshold of 10^{-3}.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	E1 Port
AID Type	E1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	T-BERL (incoming line signal BER thresholds exceeded)
Effect on Service	SA or NSA
Alarm Entity Type	E1
Description	inc. (from DSX) E1 sig. failed
Likely Cause	Failure of upstream equipment or facility (towards the DSX-1) Cross-talk in office wiring Failure of the 56DS1/E1 circuit pack
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-56: “Clear "inc. (from DSX) E1" alarms” (p. 5-142).

inc. EC1 line AIS

Description

The system has detected an EC-1 alarm indication signal (AIS) for the specified EC-1 signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	EC1 Port
AID Type	EC-1 Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	AIS (AIS detected)
Effect on Service	SA or NSA
Alarm Entity Type	EC1
Description	inc. EC1 line AIS
Likely Cause	The upstream equipment failed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-57: “Clear "inc. EC1" alarms” (p. 5-145).

inc. EC1 LOF

Description

The system has detected a loss-of-frame (LOF) condition in an incoming EC-1 signal. LOF is declared when an out-of-frame (OOF) condition (four consecutive errored STS-1 framing patterns) persists for a period of 3 ms.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	EC1 Port
AID Type	EC-1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOF (Loss of frame)
Effect on Service	SA or NSA
Alarm Entity Type	EC1
Description	inc. EC1 LOF
Likely Cause	The upstream EC1 terminal equipment failed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-57: “Clear "inc. EC1" alarms” (p. 5-145).

inc. EC1 LOS

Description

The specified EC1 port has detected at least 128 consecutive zeros in the incoming EC-1 signal, or the energy at the EC-1 input is below a preset threshold.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	EC1 Port
AID Type	EC-1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOS (Loss of signal)
Effect on Service	SA or NSA
Alarm Entity Type	EC1
Description	inc. EC1 LOS
Likely Cause	The upstream equipment either failed or was removed. Input was disconnected either at the DSX or at the Alcatel-Lucent 1665 DMX backplane.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-57: “Clear "inc. EC1" alarms” (p. 5-145).

inc. EC1 RFI-L

Description

The system has detected a line remote failure indicator (RFI-L) returned to a transmitting terminal, indicating that the receiving terminal has detected an incoming signal failure. This alarm was previously called far-end-receive-failure (FERF) and remote defect indication line (RDI-L).

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	EC1 Port
AID Type	EC-1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FERF [Line RDI-L (Far End Remote Failure)]
Effect on Service	NSA
Alarm Entity Type	EC1
Description	inc. EC1 RFI-L
Likely Cause	Alarm condition was detected at the far-end EC-1 pack.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-57: “Clear "inc. EC1" alarms” (p. 5-145).

inc. EC1 section trace identifier mismatch

Description

The network element detected a mismatch between the actual received Section Trace format/message and the provisioned expected Section Trace format/message. (The *Receive Section Trace Identifier Monitor* and *Receive Section Trace Identifier Mismatch Consequent Action* parameters are Enabled.)

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Major (MJ) NSA Default: Minor (MN)
ASAP Type	EC1 Port
AID Type	EC-1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	TIM-S (Trace Identifier Mismatch, Section)
Effect on Service	SA or NSA
Alarm Entity Type	EC1
Description	inc. EC1 section trace identifier mismatch
Likely Cause	The actual received Section Trace Format and/or Section Trace Value do not match the provisioned Expected Receive Section Trace Format and/or Expected Receive Section Trace Value parameters.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the affected circuit pack.
Action	Proceed to Procedure 5-73: "Clear "inc. section trace identifier mismatch" alarms" (p. 5-192).

inc. EC1 section trace identifier mismatch, diagnostic

Description

The network element detected a mismatch between the actual received Section Trace format/message and the provisioned expected Section Trace format/message. (The *Receive Section Trace Identifier Monitor* and *Receive Section Trace Identifier Mismatch Consequent Action* parameters are Enabled.)

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	EC1 Port
AID Type	EC-1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	TIM-S-D (Trace Identifier Mismatch, Section - Diagnostic)
Effect on Service	NSA
Alarm Entity Type	EC1
Description	inc. EC1 section trace identifier mismatch, diagnostic
Likely Cause	The actual received Section Trace Format and/or Section Trace Value do not match the provisioned Expected Receive Section Trace Format and/or Expected Receive Section Trace Value parameters.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the affected circuit pack.
Action	Proceed to Procedure 5-73: “Clear "inc. section trace identifier mismatch" alarms” (p. 5-192).

inc. EC1 sig. degrade (BER)

Description

The bit error ratio (BER) in the specified EC-1 signal exceeds the provisioned signal degrade threshold.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	EC1 Port
AID Type	EC-1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	T-BERL (incoming line signal BER thresholds exceeded)
Effect on Service	SA or NSA
Alarm Entity Type	EC1
Description	inc. EC1 sig. degrade (BER)
Likely Cause	Either a failure of a DS3/EC1 circuit pack at the near-end or a failure of the receive fiber.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-57: “Clear "inc. EC1" alarms” (p. 5-145).

inc. EC1 sig. failed (BER)

Description

The bit error ratio (BER) in the incoming EC-1 signal exceeds the provisioned failure threshold of 10^{-3} (default).

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	EC1 Port
AID Type	EC-1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	T-BERL (incoming line signal BER thresholds exceeded)
Effect on Service	SA or NSA
Alarm Entity Type	EC1
Description	inc. EC1 sig. failed (BER)
Likely Cause	Failure of the upstream equipment or facility (towards the DSX-3) Cross talk in office wiring Failure of EC-1 circuit pack (12DS3/EC1 [LNW16] or 48DS3/EC1 [LNW19/19B]).
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-57: “Clear "inc. EC1" alarms” (p. 5-145).

inc. FE-LAN ANM

Description

Incoming Auto Negotiation Mismatch (ANM) has been detected on the LAN port. This indicates that a signal has been received, but the LAN port is unable to negotiate mutually acceptable transmission options for line rate, duplex mode, and/or flow control mode.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	Fast Ethernet port
AID Type	Ethernet 10/100 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	ANM (Auto Negotiation Mismatch)
Effect on Service	SA
Alarm Entity Type	FELAN
Description	inc. FE-LAN ANM
Likely Cause	The line rate, duplex mode, and/or flow control mode on the local LAN port and the interfacing customer LAN port do not match.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-58: "Clear "inc. FE-LAN ANM" alarm" (p. 5-147).

inc. FE-LAN FEFI

Description

An incoming far end failure indication (FEFI) has been detected on the LAN port. The interfacing customer equipment has detected an incoming failure and is transmitting a far end failure indication (FEFI) downstream.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Reported (NR)
ASAP Type	Fast Ethernet port
AID Type	Ethernet 10/100 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FERF [Line RDI-L (Far End Remote Failure)]
Effect on Service	SA
Alarm Entity Type	FELAN
Description	inc. FE-LAN FEFI
Likely Cause	The interfacing customer equipment has detected an incoming failure and is transmitting a far end failure indication (FEFI) downstream.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-59: “Clear "inc. FE-LAN FEFI" alarm” (p. 5-151).

inc. FE-LAN LOS

Description

Indicates a loss of signal (LOS) at an input of the local LAN port. This condition indicates that at least 128 consecutive zeros were detected in the Ethernet signal received by the local LAN port.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	Fast Ethernet port
AID Type	Ethernet 10/100T Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOS (Loss of signal)
Effect on Service	SA
Alarm Entity Type	FELAN
Description	inc. FE-LAN LOS
Likely Cause	Disconnected LAN cable or fiber, or failure or removal of interfacing customer LAN equipment.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-60: “Clear "inc. FE-LAN LOS" alarm” (p. 5-154).

inc. GE-LAN ANM

Description

Incoming Auto Negotiation Mismatch (ANM) has been detected on the Gigabit Ethernet LAN port. This indicates that a signal has been received, but the LAN port is unable to negotiate a mutually acceptable transmission option for flow control mode.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Gigabit Ethernet port
AID Type	Ethernet 1GbE Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	ANM (Auto Negotiation Mismatch)
Effect on Service	SA or NSA
Alarm Entity Type	GELAN
Description	inc. GE-LAN ANM
Likely Cause	The flow control mode on the local LAN port and the interfacing customer LAN port do not match.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-61: “Clear "inc. GE-LAN ANM" alarm” (p. 5-156).

inc. GE-LAN LOS

Description

Loss of signal (LOS) indicates that the Gigabit Ethernet LAN port does not detect the presence of an incoming IEEE 802.3 compliant signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Gigabit Ethernet port
AID Type	Ethernet 1GbE Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOS (Loss of signal)
Effect on Service	SA or NSA
Alarm Entity Type	GELAN
Description	inc. GE-LAN LOS
Likely Cause	Disconnected LAN cable or fiber, or failure or removal of interfacing customer LAN equipment.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-62: “Clear "inc. GE-LAN LOS" alarm” (p. 5-159).

inc. LAG Partial Link Loss

Description

Transmission is lost on one link in the specified Link Aggregation Group.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	Link Aggregation Group
AID Type	LAG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	PLL (Partial Link Loss)
Effect on Service	SA
Alarm Entity Type	LAG
Description	inc. LAG Partial Link Loss
Likely Cause	Likely causes include: • Pluggable transmission module is removed or failed. • LAN loss of signal or auto negotiation mismatch is detected. • Port Administration Control parameter is disabled. • Configuration conflict with interfacing customer equipment.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-64: “Clear "inc. LAG" alarms” (p. 5-164).

inc. LAG PLCF

Description

The Link Aggregation Group is using the standard LACP protocol and one or more members of the Link Aggregation Group is not receiving standard compliant messages.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	Link Aggregation Group
AID Type	LAG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	PLCF (Partner LAG Configuration Failed)
Effect on Service	SA
Alarm Entity Type	LAG
Description	inc. LAG PLCF
Likely Cause	A configuration conflict with the interfacing customer Link Aggregation Group (LAG partner). The interfacing customer equipment may not be configured for Link Aggregation or has Link Aggregation Control Protocol (LACP) disabled.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-64: “Clear "inc. LAG" alarms” (p. 5-164).

inc. LAG Total Link Loss

Description

Transmission is lost on both links in the specified Link Aggregation Group.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	Link Aggregation Group
AID Type	LAG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	TLL (Total Link Loss)
Effect on Service	SA
Alarm Entity Type	LAG
Description	inc. LAG Total Link Loss
Likely Cause	Likely causes include: • Pluggable transmission module is removed or failed. • LAN loss of signal or auto negotiation mismatch is detected. • Port Administration Control parameter is disabled. • Configuration conflict with interfacing customer equipment. • One member LAN port is directly connected to the other.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-64: “Clear "inc. LAG" alarms” (p. 5-164).

inc. line sync. ref. OOL

Description

An off-frequency condition has been detected on the incoming OC-n line synchronization reference signal based on the frequency offset of the reference relative to the local oscillator.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Active default: Minor (MN) Standby default: Minor (MN)
ASAP Type	OCn Port
AID Type	OC-n Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SYNCOOS (Active reference off frequency) SYNC (Standby reference off frequency)
Effect on Service	NSA
Alarm Entity Type	OCn
Description	inc. line sync. ref. OOL
Likely Cause	A synchronization problem at the upstream node may cause the TX interfaces (at the upstream node) to transmit off frequency. The alarm could also be the result of an undetected hardware fault on one or both of the local main circuit packs. An incoming signal fault that interferes with clock recovery could also cause the alarm.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-63: “Clear "inc. line sync. ref. OOL" alarm” (p. 5-161).

inc. LOS

Description

Loss of signal (LOS) indicates that a Data port does not detect the presence of a valid incoming data signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Data port
AID Type	Data port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOS (Loss of signal)
Effect on Service	SA or NSA
Alarm Entity Type	DATA
Description	inc. LOS
Likely Cause	Disconnected data cable or fiber, or failure or removal of interfacing customer data equipment.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-65: “Clear "inc. LOS" alarm” (p. 5-168).

inc. Loss of Synch

Description

Indicates the loss of character synchronization on the specified Gigabit Ethernet/Data port.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Data port Gigabit Ethernet port
AID Type	Data port Gigabit Ethernet port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LSYNCH (Loss of synchronization)
Effect on Service	SA or NSA
Alarm Entity Type	DATA GELAN
Description	inc. Loss of Synch
Likely Cause	Faulty data cable/fiber/connector, or the interfacing customer equipment failed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-66: “Clear "inc. Loss of Synch" alarm” (p. 5-170).

inc. MUX OCH LOS-P

Description

The system has detected a loss of signal payload (LOS-P) condition on the incoming optical channel (OCH) port. The incoming power level of the payload signal at the receiver has dropped to a level that is causing errors.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	OCH Port
AID Type	OCH
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	MUX-LOS-P (Loss of Signal Payload in the MUX direction)
Effect on Service	SA
Alarm Entity Type	OCH
Description	inc. MUX OCH LOS-P
Likely Cause	The optical transmitter, the interconnecting fiber/connectors, or the OCH receiver failed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-67: “Clear "inc. MUX OCH LOS-P" alarm” (p. 5-172).

inc. OCN line AIS

Description

The system has detected an OC-N line alarm indication signal (AIS) on an incoming OC-3/OC-12/OC-48/OC-192 line.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Not Alarmed (NA)
ASAP Type	OCn Port
AID Type	OC-N Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	AIS (AIS detected)
Effect on Service	SA or NSA
Alarm Entity Type	OC3, OC12, OC48, or OC192
Description	inc. OC3 line AIS, inc. OC12 line AIS, inc. OC48 line AIS, or inc. OC192 line AIS
Likely Cause	The OC-N OLIU circuit pack failed at the far-end.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-68: “Clear "inc. OCN" alarms” (p. 5-176).

inc. OCN LOF

Description

The system has detected a loss-of-frame (LOF) condition in an incoming OC-N signal. LOF is declared when an out-of-frame (OOF) condition (four consecutive errored STS-1 framing patterns) persists for a period of 3 ms.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	OCn Port
AID Type	OC-N Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOF (Loss of frame)
Effect on Service	SA or NSA
Alarm Entity Type	OC3, OC12, OC48, or OC192
Description	inc. OC3 LOF, inc. OC12 LOF, inc. OC48 LOF, or inc. OC192 LOF
Likely Cause	The upstream OCN terminal equipment failed or there is incorrect OCN port provisioning at either the upstream OCN terminal equipment or the local network element. An unprotected line/port carrying service failed: SA. A protected line/port failed: NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-68: “Clear "inc. OCN" alarms” (p. 5-176).

inc. OCN LOS

Description

The system has detected a loss-of-signal (LOS) condition on the OC-3/OC-12/OC-48/OC-192 line.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	OCn Port
AID Type	OC-N Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOS (Loss of signal)
Effect on Service	SA or NSA
Alarm Entity Type	OC3, OC12, OC48, or OC192
Description	inc. OC3 LOS, inc. OC12 LOS, inc. OC48 LOS, or inc. OC192 LOS
Likely Cause	The OC-N OLIU circuit pack/pluggable transmission module failed at the near end, the receive fiber failed, or the OLIU circuit pack failed at the far end. An unprotected line/port carrying service failed: SA. A protected line/port failed: NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-68: “Clear "inc. OCN" alarms” (p. 5-176).

inc. OCN RFI-L

Description

The system has detected a line remote failure indicator (RFI-L) on an incoming OC-N line, indicating that the far-end network element has detected an incoming signal failure. This alarm was previously called far-end-receive-failure (FERF) and remote defect indication line (RDI-L).

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	OCn Port
AID Type	OC-N Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FERF [Line RDI-L (Far End Remote Failure)]
Effect on Service	NSA
Alarm Entity Type	OC3, OC12, OC48, or OC192
Description	inc. OC3 RFI-L, inc. OC12 RFI-L, inc. OC48 RFI-L, or inc. OC192 RFI-L
Likely Cause	An incoming signal failure was detected at the far-end network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-69: “Clear "inc. OCN RFI-L" alarm” (p. 5-180).

inc. OCN section trace identifier mismatch

Description

The network element detected a mismatch between the actual received Section Trace format/message and the provisioned expected Section Trace format/message. (The *Receive Section Trace Identifier Monitor* and *Receive Section Trace Identifier Mismatch Consequent Action* parameters are Enabled.)

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Major (MJ) NSA Default: Minor (MN)
ASAP Type	OCN Port
AID Type	OC-N Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	TIM-S (Trace Identifier Mismatch, Section)
Effect on Service	SA or NSA
Alarm Entity Type	OCN
Description	inc. OCN section trace identifier mismatch
Likely Cause	The actual received Section Trace Format and/or Section Trace Value do not match the provisioned Expected Receive Section Trace Format and/or Expected Receive Section Trace Value parameters.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the affected circuit pack.
Action	Proceed to Procedure 5-73: “Clear "inc. section trace identifier mismatch" alarms” (p. 5-192).

inc. OCN section trace identifier mismatch, diagnostic

Description

The network element detected a mismatch between the actual received Section Trace format/message and the provisioned expected Section Trace format/message. (The *Receive Section Trace Identifier Monitor* and *Receive Section Trace Identifier Mismatch Consequent Action* parameters are Enabled.)

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	OCN Port
AID Type	OC-N Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	TIM-S-D (Trace Identifier Mismatch, Section - Diagnostic)
Effect on Service	NSA
Alarm Entity Type	OCN
Description	inc. OCN section trace identifier mismatch, diagnostic
Likely Cause	The actual received Section Trace Format and/or Section Trace Value do not match the provisioned Expected Receive Section Trace Format and/or Expected Receive Section Trace Value parameters.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the affected circuit pack.
Action	Proceed to Procedure 5-73: “Clear "inc. section trace identifier mismatch" alarms” (p. 5-192).

inc. OCN sig. degrade (BER)

Description

The bit error ratio (BER) in the specified OC-N signal exceeds the provisioned signal degrade threshold.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	OCn Port
AID Type	OC-N Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	T-BERL (incoming line signal BER thresholds exceeded)
Effect on Service	SA or NSA
Alarm Entity Type	OC3, OC12, OC48, or OC192
Description	inc. OC3 sig. degrade (BER), inc. OC12 sig. degrade (BER), inc. OC48 sig. degrade (BER), or inc. OC192 sig. degrade (BER)
Likely Cause	The OC-N OLIU circuit pack failed at the near end, the receive fiber failed, or the OLIU circuit pack failed at the far end, or there is a problem with the optical attenuator usage. An unprotected line/port carrying service failed: SA. A protected line/port failed: NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-68: “Clear "inc. OCN" alarms” (p. 5-176).

inc. OCN sig. failed (BER)

Description

The bit error ratio (BER) in the incoming OC-N signal exceeds the provisioned failure threshold of 10^{-3} (default).

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	OCn Port
AID Type	OC-N Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	T-BERL (incoming line signal BER thresholds exceeded)
Effect on Service	SA or NSA
Alarm Entity Type	OC3, OC12, OC48, or OC192
Description	inc. OC3 sig. failed, inc. OC12 sig. failed, inc. OC48 sig. failed, or inc. OC192 sig. failed
Likely Cause	The OC-N OLIU circuit pack failed at the near end, the receive fiber failed, or the OLIU circuit pack failed at the far end. An unprotected line/port carrying service failed: SA. A protected line/port failed: NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-68: "Clear "inc. OCN" alarms" (p. 5-176).

inc. ODU2 BDI

Description

The system has detected a backward defect indicator (BDI) on an incoming 10G optical channel data unit (ODU2) signal (from the OTU2 port), indicating that the far-end network element has detected an incoming ODU2 signal failure.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	ODU2 Tributary
AID Type	ODU2 Tributary
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	BDI (Backward Defect Indication)
Effect on Service	NSA
Alarm Entity Type	ODU2
Description	inc. ODU2 BDI
Likely Cause	An incoming ODU2 signal failure was detected at the far-end network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-11: “Clear "inc. BDI" alarms” (p. 5-38).

inc. ODU2 DEG

Description

The bit error ratio (BER) based on bit interleaved parity 8 (BIP-8) violations in the incoming 10G optical channel data unit (ODU2) signal (from the OTU2 port) exceeds the threshold.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	ODU2 Tributary
AID Type	ODU2 Tributary
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	DEG (Degraded Signal)
Effect on Service	SA or NSA
Alarm Entity Type	ODU2
Description	inc. ODU2 DEG
Likely Cause	The XM10G/8 circuit pack failed at the near end, the receive fiber failed, or the XM10G/8 circuit pack failed at the far end, or there is a problem with the optical attenuator usage. SA when the OTU2 is the destination of an OCH cross-connection and at least one of the client ports has a Signal Type of other than STNA. Otherwise, the alarm is reported as NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-71: “Clear "inc. ODU2/OTU2" alarms” (p. 5-185).

inc. ODU2 LCK

Description

The system has detected a locked (LCK) maintenance signal on an incoming 10G optical channel data unit (ODU2) signal (from the OTU2 port). This indicates that an upstream connection is administratively locked and no signal is passed through.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	ODU2 Tributary
AID Type	ODU2 Tributary
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LCK (Lock Signal)
Effect on Service	SA or NSA
Alarm Entity Type	ODU2
Description	inc. ODU2 LCK
Likely Cause	An upstream network element has administratively locked the ODU2 signal from user access while performing a maintenance activity (for example, set-up tests). SA when the OTU2 is the destination of an OCH cross-connection and at least one of the client ports has a Signal Type of other than STNA. Otherwise, the alarm is reported as NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-70: “Clear "inc. ODU2 LCK/OCI" alarms” (p. 5-184).

inc. ODU2 OCI

Description

The system has detected a open connection indication (OCI) maintenance signal on an incoming 10G optical channel data unit (ODU2) signal (from the OTU2 port). This indicates that an upstream connection is not connected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	ODU2 Tributary
AID Type	ODU2 Tributary
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	OCI (Open Connection Indication)
Effect on Service	SA or NSA
Alarm Entity Type	ODU2
Description	inc. ODU2 OCI
Likely Cause	An input port is not connected to an output port at an upstream network element (optical cross-connect/switching fabric). SA when the OTU2 is the destination of an OCH cross-connection and at least one of the client ports has a Signal Type of other than STNA. Otherwise, the alarm is reported as NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-70: "Clear "inc. ODU2 LCK/OCI" alarms" (p. 5-184).

inc. ODU2 SSF

Description

The system has detected a server signal failure (SSF) on an incoming 10G optical channel data unit (ODU2) signal (from the OTU2 port). An ODU2 SSF maintenance signal alerts the client (ODU2) that the server (OTU2) has detected an OTU2 defect.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	ODU2 Tributary
AID Type	ODU2 Tributary
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SSF (Signal Server Fail)
Effect on Service	SA or NSA
Alarm Entity Type	ODU2
Description	inc. ODU2 SSF
Likely Cause	An OTU2 AIS, LOF, or LOM condition exists or an ODU2 AIS is detected. SA when the OTU2 is the destination of an OCH cross-connection and at least one of the client ports has a Signal Type of other than STNA. Otherwise, the alarm is reported as NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-71: “Clear "inc. ODU2/OTU2" alarms” (p. 5-185).

inc. OTS LOS-P

Description

The system has detected a loss of signal payload (LOS-P) condition on the OTS line.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	OTS Port
AID Type	OTS Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOS-P (Loss of Signal Payload)
Effect on Service	SA or NSA
Alarm Entity Type	OTS
Description	inc. OTS LOS-P
Likely Cause	The far-end OTS transmitter, the interconnecting fiber/connectors, or the OTS receiver failed. SA when at least one of its OCH ports is the source of an OCH cross-connection. Otherwise, the alarm is reported as NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-72: “Clear "inc. OTS LOS-P" alarm” (p. 5-189).

inc. OTU2 BDI

Description

The system has detected a backward defect indicator (BDI) on an incoming 10G optical channel transport unit (OTU2) signal, indicating that the far-end network element has detected incoming OTU2 signal failure.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	OTU2 Port
AID Type	OTU2 port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	BDI (Backward Defect Indication)
Effect on Service	NSA
Alarm Entity Type	OTU2
Description	inc. OTU2 BDI
Likely Cause	An incoming OTU2 signal failure was detected at the far-end network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-11: “Clear "inc. BDI" alarms” (p. 5-38).

inc. OTU2 DEG

Description

The bit error ratio (BER) based on bit interleaved parity 8 (BIP-8) violations in the incoming 10G optical channel transport unit (OTU2) signal exceeds the threshold.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	OTU2 Port
AID Type	OTU2 port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	DEG (Degraded signal)
Effect on Service	SA or NSA
Alarm Entity Type	OTU2
Description	inc. OTU2 DEG
Likely Cause	The XM10G/8 circuit pack failed at the near end, the receive fiber failed, or the XM10G/8 circuit pack failed at the far end, or there is a problem with the optical attenuator usage. SA when the OTU2 is the destination of an OCH cross-connection and at least one of the client ports has a Signal Type of other than STNA. Otherwise, the alarm is reported as NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-71: “Clear "inc. ODU2/OTU2" alarms” (p. 5-185).

inc. OTU2 LOF

Description

The system has detected a loss-of-frame (LOF) condition in an incoming OTU2 signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	OTU2 Port
AID Type	OTU2 port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOF (Loss of frame)
Effect on Service	SA or NSA
Alarm Entity Type	OTU2
Description	inc. OTU2 LOF
Likely Cause	The far-end OTU2 terminating equipment failed. SA when the OTU2 is the destination of an OCH cross-connection and at least one of the client ports has a Signal Type of other than STNA. Otherwise, the alarm is reported as NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-71: “Clear "inc. ODU2/OTU2" alarms” (p. 5-185).

inc. OTU2 LOM

Description

The system has detected a loss-of-multiframe (LOM) condition in an incoming OTU2 signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	OTU2 Port
AID Type	OTU2 port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOM (Loss of Multiframe)
Effect on Service	SA or NSA
Alarm Entity Type	OTU2
Description	inc. OTU2 LOM
Likely Cause	The far-end OTU2 terminating equipment failed. SA when the OTU2 is the destination of an OCH cross-connection and at least one of the client ports has a Signal Type of other than STNA. Otherwise, the alarm is reported as NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-71: “Clear "inc. ODU2/OTU2" alarms” (p. 5-185).

inc. OTU2 LOS-P

Description

The system has detected a loss of signal payload (LOS-P) condition on the incoming OTU2 line.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	OTU2 Port
AID Type	OTU2 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOS-P (Loss of Signal Payload)
Effect on Service	SA or NSA
Alarm Entity Type	OTU2
Description	inc. OTU2 LOS-P
Likely Cause	The far-end OTU2 transmitter, the interconnecting fiber/connectors, or the OTU2 receiver failed. SA when the OTU2 is the destination of an OCH cross-connection and at least one of the client ports has a Signal Type of other than STNA. Otherwise, the alarm is reported as NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-71: “Clear "inc. ODU2/OTU2" alarms” (p. 5-185).

inc. OTU2 SSF

Description

The system has detected a server signal failure (SSF) condition on an incoming 10G optical channel transport unit (OTU2) signal resulting from an incoming OTU2 LOS or AIS insertion.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	OTU2 Port
AID Type	OTU2 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SSF (Signal Server Fail)
Effect on Service	SA or NSA
Alarm Entity Type	OTU2
Description	inc. OTU2 SSF
Likely Cause	The OTU2 SSF is a consequent action of an OTU2 LOS or AIS insertion in the incoming OTU2 signal. SA when the OTU2 is the destination of an OCH cross-connection and at least one of the client ports has a Signal Type of other than STNA. Otherwise, the alarm is reported as NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-71: “Clear "inc. ODU2/OTU2" alarms” (p. 5-185).

inc. STS LOP

Description

The system has detected an incoming loss-of-pointer (LOP) condition. A valid pointer could not be found for eight consecutive frames in the identified incoming EC-1 signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	STS Ring Channel
AID Type	STS Ring Channel within an EC-1
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOP (Loss of pointer)
Effect on Service	SA or NSA
Alarm Entity Type	STS1
Description	inc. STS LOP
Likely Cause	A circuit pack failed at the near-end or far-end of the line. If the condition affects the same pointer in both lines of an interface, the cause could be unprotected failure of an STS cross-connected circuit pack (EC-1) in the adjacent upstream network element or a cross-connection mismatch between STS-1s. An unprotected circuit pack carrying service failed - SA. A protected circuit pack failed - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-57: “Clear "inc. EC1" alarms” (p. 5-145).

inc. STSN AIS

Description

The system has detected an incoming STS-N alarm indication signal (AIS) in an OC-3/OC-12/OC-12/OC-48/OC-192 or EC-1 line.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	STS Ring Channel
AID Type	STS-1, STS-3c, STS-12c, STS-48c, or STS-192c Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	AIS (AIS detected)
Effect on Service	SA or NSA
Alarm Entity Type	STS1, STS3C, STS12C, STS48C, or STS192C
Description	inc. STS1 AIS, inc. STS3C AIS, inc. STS12C AIS, inc. STS48C AIS, or inc. STS192C AIS
Likely Cause	Incomplete or incorrect cross-connect provisioning in an end-to-end network; unprotected removal or failure of a low-speed circuit pack at the far-end; unprotected optical line failure.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-74: “Clear "inc. STSN" conditions/alarms” (p. 5-195).

inc. STSN LOP

Description

The system has detected a loss-of-pointer (LOP) condition. A valid STS-N pointer could not be found for eight consecutive frames in the identified STS-N signal.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	STS Ring Channel
AID Type	STS-1, STS-3c, STS-12c, STS-48c, or STS-192c Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOP (Loss of pointer)
Effect on Service	SA or NSA
Alarm Entity Type	STS1, STS3C, STS12C, STS48C, or STS192C
Description	inc. STS1 LOP, inc. STS3C LOP, inc. STS12C LOP, inc. STS48C LOP, or inc. STS192C LOP
Likely Cause	If this condition occurs on only one OC-N line, the likely cause is a failed OC-N OLIU circuit pack at the near-end or far-end of the line. If the condition affects the same pointer in both OC-N lines of an OC-N interface, the cause could be unprotected failure of an STS cross-connected circuit pack (DS3) in the adjacent upstream network element or cross-connect mismatch between STS-1, STS-3c, STS-12c, STS-48c, and STS-192c. An unprotected line/port carrying service failed: SA. A protected line/port failed: NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-74: “Clear "inc. STSN" conditions/alarms” (p. 5-195).

inc. STSN RFI-P

Description

The system has detected an STS path remote failure indicator (RFI-P) indicating that the receiving terminal has detected an incoming signal failure. This alarm was previously called Yellow (YEL) and remote defect indication path (RFI-P).

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	STS Ring Channel
AID Type	STS-1, STS-3c, STS-12c, STS-48c, or STS-192c Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	YEL (Yellow Alarm - RDI-P)
Effect on Service	NSA
Alarm Entity Type	STS1, STS3C, STS12C, STS48C, or STS192C
Description	inc. STS1 RFI-P, inc. STS3C RFI-P, inc. STS12C RFI-P, inc. STS48C RFI-P, or inc. STS192C RFI-P
Likely Cause	An upstream STS-N cross-connect has been deleted; an upstream failure (for example, LOS or LOF) has been detected.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-74: “Clear "inc. STSN" conditions/alarms” (p. 5-195).

inc. STSN sig. degrade (BER)

Description

For STS-N path switched ring applications, the bit error ratio (BER) of the specified STS-N signal exceeds the provisioned signal degrade threshold.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	STS Ring Channel
AID Type	STS-1, STS-3c, STS-12c, STS-48c, or STS-192c Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	T-BERP (incoming ring path signal BER thresholds exceeded)
Effect on Service	SA or NSA
Alarm Entity Type	STS1, STS3C, STS12C, STS48C, or STS192C
Description	inc. STS1 sig. degrade (BER), inc. STS3C sig. degrade (BER), inc. STS12C sig. degrade (BER), inc. STS48C sig. degrade (BER), or inc. STS192C sig. degrade (BER)
Likely Cause	Fiber failed or an OC-N OLIU circuit pack failed at some point in the STS-N path. An unprotected line/port carrying service failed: SA. A protected line/port failed: NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-74: “Clear "inc. STSN" conditions/alarms” (p. 5-195).

inc. STSN sig. failed (BER)

Description

For STS-N path switched ring applications, the bit error ratio (BER) of the specified STS-N signal exceeds the provisioned soft error threshold of 10^{-3} (default).

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	STS Ring Channel
AID Type	STS-1, STS-3c, STS-12c, STS-48c, or STS-192c Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	T-BERP (incoming ring path signal BER thresholds exceeded)
Effect on Service	SA or NSA
Alarm Entity Type	STS1, STS3C, STS12C, STS48C, or STS192C
Description	inc. STS1 sig. failed (BER), inc. STS3C sig. failed (BER), inc. STS12C sig. failed (BER), inc. STS48C sig. failed (BER), or inc. STS192C sig. failed (BER)
Likely Cause	The near-end OC-N OLIU circuit pack failed, the far-end OLIU failed, the receive fiber failed if the OC-N is also reporting a failure, or a nonadjacent fiber failed in the receive path. An unprotected circuit pack failed - SA. A protected circuit pack failed - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-74: “Clear "inc. STSN" conditions/alarms” (p. 5-195).

inc. STSN unequipped

Description

The system has detected the unequipped code (SONET path overhead signal code label byte=0) on an in-service STS-N channel.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	STS Ring Channel
AID Type	STS-1, STS-3c, STS-12c, STS-48c, or STS-192c Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SLMF (Signal Label Mismatch Failure)
Effect on Service	SA or NSA
Alarm Entity Type	STS1, STS3C, STS12C, STS48C, or STS192C
Description	inc. STS1 unequipped, inc. STS3C unequipped, inc. STS12C unequipped, inc. STS48C unequipped, or inc. STS192C unequipped
Likely Cause	An upstream STS-N cross-connect error was made or a cross-connect was deleted. An unprotected circuit pack failed - SA. A protected circuit pack failed - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-74: “Clear "inc. STSN" conditions/alarms” (p. 5-195).

inc. VCG failed

Description

Indicates a failure condition in an incoming virtual concatenation group (VCG). The failure of any VT1.5 or STSN tributary in the VCG causes a VCG failure.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	VCG Port
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOS (Loss of signal)
Effect on Service	SA or NSA
Alarm Entity Type	VCG
Description	inc. VCG failed
Likely Cause	Cross-connection error in one or more VT1.5 or STSN tributaries in the VCG.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-75: “Clear "inc. VCG failed" alarm” (p. 5-199).

inc. VCG LFD

Description

A loss of frame delineation (LFD) has been detected in an incoming virtual concatenation group (VCG).

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	MISC (Miscellaneous condition)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	VCG
Description	inc. VCG LFD
Likely Cause	The far end Ethernet circuit pack does not support the ITU-T G.7041/Y.1303 Generic framing procedure (GFP).
Visible Indication	None
Action	Proceed to Procedure 5-76: “Clear "inc. VCG LFD" condition” (p. 5-203).

inc. VCG LOA

Description

One or more VT1.5 or STSN tributaries that compose a virtual concatenation group (VCG) are out of multiframe alignment because of an excess delay difference.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	MISC (Miscellaneous condition)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	VCG
Description	inc. VCG LOA
Likely Cause	A VT1.5 or STSN tributary in the VCG is routed over a path that exceeds the allowed delay difference.
Visible Indication	None
Action	Proceed to Procedure 5-77: “Clear "inc. VCG LOA" condition” (p. 5-206).

inc. VC TU-AIS

Description

The system has detected a virtual container tributary unit (TU) alarm indication signal (AIS) incoming from the active OC-N line. The system responds by transmitting AIS toward the DSX-1 and a Remote Defect Indication (RDI) signal back toward the fiber where the AIS is being received.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	VC12 Ring Channel
AID Type	VC-12 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	AIS (AIS detected)
Effect on Service	SA
Alarm Entity Type	VC12
Description	inc. VC TU-AIS
Likely Cause	Incomplete or incorrect cross-connect provisioning in end-to-end network; unprotected removal or failure of a DS1/E1 circuit pack at the far-end. In ring applications, a non-service affecting VC TU-AIS alarm message may result from an upstream OLIU or fiber failure affecting only one ring direction. An RDI signal is not returned for a non-service affecting VC TU-AIS.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-78: “Clear "inc. VC" conditions/alarms” (p. 5-208).

inc. VC TU-LOP

Description

The system has detected a virtual container tributary unit loss-of-pointer (LOP) condition. TU-LOP is derived by monitoring the TU overhead bytes V1 and V2. The system responds by transmitting AIS toward the DSX-1 and a Remote Defect Indication (RDI) signal back toward the fiber where the signal is being received.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	VC12 Ring Channel
AID Type	VC-12 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOP (Loss of pointer)
Effect on Service	SA
Alarm Entity Type	VC12
Description	inc. VC TU-LOP
Likely Cause	Unprotected failure of the OC-N OLIU at the near end; failure of an OLIU or DS1/E1 circuit pack at the far end. An unprotected circuit pack failed - SA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-78: “Clear "inc. VC" conditions/alarms” (p. 5-208).

inc. VC LP-RFI

Description

The system has detected a Remote Defect Indication (RDI) signal that has persisted continuously for approximately 2.5 seconds.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	VC12 Ring Channel
AID Type	VC-12 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	YEL (Yellow Alarm - RDI-P)
Effect on Service	NSA
Alarm Entity Type	VC12
Description	inc. VC LP-RFI
Likely Cause	Alarm condition was detected at the far-end OLIU.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-78: "Clear "inc. VC" conditions/alarms" (p. 5-208).

inc. VC unequipped

Description

The system has detected five consecutive unequipped frames. The system transmits AIS toward the DSX-1.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	VC12 Ring Channel
AID Type	VC-12 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SLMF (Signal Label Mismatch Failure)
Effect on Service	SA
Alarm Entity Type	VC12
Description	inc. VC unequipped
Likely Cause	An upstream cross-connect has been deleted. An unprotected circuit pack failed - SA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-78: “Clear "inc. VC" conditions/alarms” (p. 5-208).

inc. VT AIS

Description

The system has detected a virtual tributary (VT) path alarm indication signal (AIS) incoming from the active OC-N line. The system responds by transmitting DS1 AIS toward the DSX-1 and VT RFI-V back toward the fiber where the AIS is being received.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Major (MJ) NSA Default: Minor (MN)
ASAP Type	VT1.5 Ring Channel
AID Type	VT1.5 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	AIS (AIS detected)
Effect on Service	SA or NSA
Alarm Entity Type	VT1
Description	inc. VT AIS
Likely Cause	Incomplete or incorrect cross-connect provisioning in end-to-end network; unprotected removal or failure of a DS1 circuit pack at the far-end. In ring applications, a non-service affecting VT AIS alarm message may result from an upstream OLIU or fiber failure affecting only one ring direction. A VT RFI-V alarm message is not returned for a non-service affecting VT AIS.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-79: “Clear "inc. VT" conditions/alarms” (p. 5-212).

inc. VT LOP

Description

The system has detected a virtual tributary (VT) loss-of-pointer (LOP) condition. A valid VT pointer could not be found for eight consecutive frames in the identified virtual channel.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Major (MJ) NSA Default: Minor (MN)
ASAP Type	VT1.5 Ring Channel
AID Type	VT1.5 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LOP (Loss of pointer)
Effect on Service	SA or NSA
Alarm Entity Type	VT1
Description	inc. VT LOP
Likely Cause	Unprotected failure of the OC-N OLIU at the near end; failure of an OLIU or DS1 circuit pack at the far end. An unprotected circuit pack failed - SA. A protected circuit pack failed - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-79: “Clear "inc. VT" conditions/alarms” (p. 5-212).

inc. VT RFI-V

Description

The system has detected a virtual tributary (VT) remote failure indicator (RFI-V) indicating that the receiving terminal has detected an incoming signal failure. This alarm was previously called Yellow (YEL) and remote defect indication VT (RFI-V).

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	VT1.5 Ring Channel
AID Type	VT1.5 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	YEL (Yellow Alarm - RDI-P)
Effect on Service	NSA
Alarm Entity Type	VT1
Description	inc. VT RFI-V
Likely Cause	Alarm condition was detected at the far-end OLIU.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-79: “Clear "inc. VT" conditions/alarms” (p. 5-212).

inc. VT sig. degrade (BER)

Description

In a virtual tributary (VT) path switched ring, the system has detected a VT error rate that exceeds the provisioned signal degrade threshold.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Major (MJ) NSA Default: Minor (MN)
ASAP Type	VT1.5 Ring Channel
AID Type	VT1.5 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	T-BERP (incoming ring path signal BER thresholds exceeded)
Effect on Service	SA or NSA
Alarm Entity Type	VT1
Description	inc. VT sig. degrade (BER)
Likely Cause	An OC-N OLIU circuit pack failure or a fiber failure at some point on the failed ring. An unprotected circuit pack failed - SA. A protected circuit pack failed - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-79: “Clear "inc. VT" conditions/alarms” (p. 5-212).

inc. VT unequipped

Description

The system has detected the unequipped code (SONET path overhead VT signal code label byte=0) on an in-service VT1.5 channel.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Major (MJ) NSA Default: Minor (MN)
ASAP Type	VT1.5 Ring Channel
AID Type	VT1.5 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SLMF (Signal Label Mismatch Failure)
Effect on Service	SA or NSA
Alarm Entity Type	VT1
Description	inc. VT unequipped
Likely Cause	An upstream VT1.5 cross-connect has been deleted. An unprotected circuit pack failed - SA. A protected circuit pack failed - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-79: "Clear "inc. VT" conditions/alarms" (p. 5-212).

incoming CRC-4 MFA mismatch

Description

Indicates a difference between the signal format of the incoming E1 signal (from the DSX) and the provisioned signal format of the receiving E1 port.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	E1 Port
AID Type	E1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	CRCMM (CRC-4 Multiframe Alignment Mismatch)
Effect on Service	NSA
Alarm Entity Type	E1
Description	incoming CRC-4 MFA mismatch
Likely Cause	The E1 port is provisioned to receive CRC-4 formatted E1 signals, and the incoming E1 signal is a non-CRC-4 formatted E1 signal.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-80: "Clear "incoming CRC-4 MFA mismatch" condition" (p. 5-216).

incompatible CP version

Description

An older version of a large fabric Main was inserted into a slot that contained a newer version of the same large fabric Main.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	NSA
Alarm Entity Type	EQPT
Description	incompatible CP version
Likely Cause	An older version of a large fabric Main was inserted into a slot that contained a newer version of the same large fabric Main.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the affected circuit pack.
Action	Proceed to Procedure 5-81: “Clear "incompatible CP version" alarm” (p. 5-218).

Inconsistent APS Codes

Description

In bidirectional line-switched rings (BLSRs), there is a rolling window of 12 frames in which 3 consecutive frames must have identical K-bytes. If this requirement is violated, an inconsistent APS codes alarm is generated.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	BLSR Protection Group
AID Type	OC-48 line OC-192 line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	APSC (APS codes inconsistent)
Effect on Service	NSA
Alarm Entity Type	OC48 OC192
Description	Inconsistent APS Codes
Likely Cause	A node in the BLSR is isolated due to • A fiber cut • An OC-48/OC-192 OLIU circuit pack failure • A SYSCTL circuit pack failure, reset, or initialization • An inc. OC-48/OC-192 sig. degrade alarm at some point on the BLSR.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-82: “Clear "Inconsistent APS Codes" alarm” (p. 5-219).

Inconsistent crs map

Description

The network element detected a corrupted cross-connection map during start up.

Alarm Data	Value/Meaning
Severity Levels	Minor (MN)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	CONTR (Control processor failure)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Inconsistent crs map
Likely Cause	The network element cross-connection map is corrupted.
Visible Indication	Lighted **MN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-83: “Clear "Inconsistent crs map" alarm” (p. 5-223).

inconsistent DCC values

Description

The "User/Network" parameter values are set the same at both ends of the DCC.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	OCn Port
AID Type	Section Data Communications Channel (DCC)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	OSILINKERR (OSI stack error, Data Link Layer)
Effect on Service	NSA
Alarm Entity Type	COM
Description	inconsistent DCC values
Likely Cause	Fibers are misconnected or user network parameter was incorrectly provisioned.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-84: "Clear "inconsistent DCC values" alarm" (p. 5-224).

Inconsistent Ring Prot Mode

Description

Some nodes in the BLSR are provisioned to UPSR.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	BLSR Protection Group
AID Type	BLSR protection group
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RNG-IRPM (Inconsistent Ring Protection Mode)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Inconsistent Ring Prot Mode
Likely Cause	A network element that is provisioned not as a BLSR was added to the BLSR ring map.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-85: “Clear "Inconsistent Ring Prot Mode" alarm” (p. 5-226).

Inconsistent VT BLSR Access

Description

A VT1.5 rate BLSR cross-connection or a VT-accessed STS-1 pass through cross-connection has been provisioned at the local node and there are nodes in the BLSR that do not support VT access.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	BLSR protection group
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RNG-IVTBA (BLSR Ring - Inconsistent VT BLSR Access)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	Inconsistent VT BLSR Access
Likely Cause	User provisioned a VT1.5 rate BLSR cross-connection or a VT-accessed STS-1 pass through cross-connection at the local node and there are other nodes in the BLSR that do not recognize/support VT access.
Visible Indication	Lighted ABN LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-86: “Clear "Inconsistent VT BLSR Access" condition” (p. 5-227).

inhibit switch

Description

Protection switching is inhibited; the active and protection states of a 1+1 protected equipment pair cannot be changed. This alarm also indicates that automatic synchronization reference switching is inhibited.

Alarm Data	Value/Meaning
Severity Levels	Slot: Not Alarmed (NA) Synch reference (external): Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	Synch reference (external): System Timing
AID Type	Slot Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	Slot: INHSWPR (Inhibited switch to protection) WKSWPR-1 (Working facility/equipment switched to protection unit 1) WKSWPR-2 (Working facility/equipment switched to protection unit 2) Synch reference (external): INHSWPR (Inhibited switch to protection)
Effect on Service	Slot: Standing Condition (SC) Synch reference (external): NSA
Alarm Entity Type	Slot: EQPT Synch reference (external): T1, E1
Description	inhibit switch
Likely Cause	User selected **Fault** → **Protection Switch** and highlighted a 1+1 Equip Protection Group and provisioned the Switch Type as **Inhibit**. User selected **Fault** → **Timing/Sync Protection Switch** → **System Timing Reference/Source Switch** and the Switch Command **Inhibit**.

Alarm Data	Value/Meaning
Visible Indication	Slot: Lighted **ABN** LED on the SYSCTL faceplate. Synch reference (external): Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-87: "Clear "inhibit switch" condition" (p. 5-230).

install failed

Description

A firmware upgrade failed on the specified circuit pack.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	install failed
Likely Cause	User selected **Configuration** → **Software** → **Apply Software** and the software apply operation did not complete successfully.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-88: “Clear "install failed" condition” (p. 5-231).

install program IP

Description

A new software generic is currently being applied to the circuit pack.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	Blank AID = SWFTDWN (Software Download) Slot AID = EOC (EOC failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	install program IP
Likely Cause	User selected **Configuration** → **Software** → **Apply Software**.
Visible Indication	None
Action	No action is necessary. The condition clears when apply is complete.

Invalid Database

Description

The system has detected no valid database on any NVM.

Alarm Data	Value/Meaning
Severity Levels	Minor (MN)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	DATAFLT (Data Integrity Fault)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Invalid Database
Likely Cause	The database version does not match the generic version, the databases are corrupted, or the MAC addresses in the database do not match the MAC addresses in the Main circuit packs.
Visible Indication	Lighted **MN** LED on the SYSCTL faceplate
Action	Proceed to Procedure 5-44: “Clear "Generic/Database/Equipment Configuration" alarms/conditions” (p. 5-104).

Invalid Subshelf Configuration

Description

During the shelf startup procedure, a shelf in a multi-shelf DCS system has detected a corrupt or missing subshelf configuration file (ssconfig.dat) on both NVMs. The `Invalid Subshelf Configuration` alarm is only reported in the maintenance mode.

Alarm Data	Value/Meaning
Severity Levels	Minor (MN)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	DATAFLT (Data Integrity Fault)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Invalid Subshelf Configuration
Likely Cause	A shelf in a multi-shelf DCS system has detected a corrupt or missing subshelf configuration file (ssconfig.dat) on both NVMs.
Visible Indication	Lighted **MN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-135: “Clear "Subshelf-related" alarms/conditions” (p. 5-329).

Line Automatic Switch

Description

An automatic BLSR protection switch occurred in response to a signal degrade or failed condition.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OC-48 line OC-192 line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LAS (Line Automatic Switch)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	OC48 OC192
Description	Line Automatic Switch
Likely Cause	An inc. OC-48/OC-192 sig. degrade or inc. OC-48/OC-192 sig. failed alarm was detected at some point on the BLSR.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-89: “Clear "Line Automatic Switch" condition” (p. 5-234).

line DCC channel failed

Description

The system cannot communicate with the far-end system through the SONET line data communications channel (DCC).

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	OCn Port
AID Type	Data Communications Channel (DCC)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC-L (line DCC channel failed)
Effect on Service	NSA
Alarm Entity Type	COM
Description	line DCC channel failed
Likely Cause	SYSCTL circuit pack failed, reset, or initialized at the far-end network element. The program installation failed at the far-end network element. The program installation is in progress at the far-end network element. The OC-N OLIU circuit pack failed at the near-end or far-end network element.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-90: “Clear "line DCC channel failed" alarm” (p. 5-237).

lockout of protection

Description

Selection of the protection line of the 1+1, 1+1_BIDIR, or 1+1_OPTM protected OC-N line or protection path (STS or VT) of a path switched ring is prevented, until the condition is cleared. If the protection tributaries are currently selected when this request is issued, traffic switches back to the service tributaries.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OC-3, OC-12, OC-48, OC-192 line STS-1, STS-3c, STS-12c, STS-48c, or STS-192c Ring Channel VT1.5 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	INHSWPR (Inhibited switch to protection)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	OC3, OC12, OC48, OC192 STS1, STS3C, STS12C,STS48C, or STS192C VT1
Description	lockout of protection
Likely Cause	User selected **Fault** → **Protection Switch** and highlighted 1+1 Line, 1+1_BIDIR Line, 1+1_OPTM Line, or Path Protection Group, and provisioned the Switch Type as **Lockout**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-91: “Clear "lockout of protection" condition” (p. 5-243).

Lockout Switch

Description

Selection of the protection tributaries (in the specified direction [East or West] on the 2-fiber BLSR) is prevented, until the conditioned is cleared. If the protection tributaries are currently selected when this request is issued, traffic switches back to the service tributaries.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OC-48 line OC-192 line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPS (Lockout Switch)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	OC48 OC192
Description	Lockout Switch
Likely Cause	User executed a manual switch on the 2-fiber BLSR using **Fault** → **Protection Switch** and selected Lockout Of Protection, Span.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-92: “Clear "Lockout Switch" condition” (p. 5-244).

lockout switching

Description

Protection switching on the 1+1_OPTM protected OC-N line is prevented, until the condition is cleared. Even if the protection line is currently selected when this request is issued, traffic freezes on the currently active line.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OC-3, OC-12, OC-48, OC-192 line (1+1 optimized protection group)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	GP (A protection switch request changed)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	OC3, OC12, OC48, OC192
Description	lockout switch
Likely Cause	User selected **Fault** → **Protection Switch** and highlighted 1+1_OPTM Line Protection Group, and provisioned the Switch Type as **Lockout**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-93: “Clear "lockout switching" condition” (p. 5-245).

Maintenance Mode

Description

The system cannot determine which generic or database to use and has entered the Maintenance mode.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	DATAFLT (Data Integrity Fault)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	Maintenance Mode
Likely Cause	The generic is not valid, the database is not valid, or there are multiple valid generics and/or databases. At least one other alarm/standing condition is also reported indicating why maintenance mode was entered.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate. The **IND** display scrolls *MPx.x* where *x.x* is the generic number.
Action	Proceed to Procedure 5-44: “Clear "Generic/Database/Equipment Configuration" alarms/conditions” (p. 5-104).

manual reference switch

Description

A user-initiated manual protection switch on line timing references.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OC-3 line OC-12 line OC-48 line OC-192 line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	WKSWPR-1 (Working facility/equipment switched to protection unit 1) WKSWPR-2 (Working facility/equipment switched to protection unit 2)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	OC3 OC12 OC48 OC192
Description	manual reference switch
Likely Cause	User selected **Fault** → **Timing/Sync Protection Switch** → **System Timing Reference/Source Switch** and the Switch Command **Manual**. The synchronization reference protection switching has been provisioned to revertive.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-94: "Clear "manual reference switch" condition" (p. 5-246).

manual switch

Description

A user-initiated manual switch has been performed on an OC-N line, RPR protection group, path switched ring, or external synchronization reference. The manual switch has not been cleared or overridden.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OC-3, OC-12, OC-48, OC-192 line STS-1, STS-3c, STS-12c, STS-48c, or STS-192c Ring Channel VT1.5 Ring Channel VCG Synch reference (external)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	WKSWPR-1 (Working facility/equipment switched to protection unit 1) WKSWPR-2 (Working facility/equipment switched to protection unit 2) MSR (VCG) (Manual switch)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	OC3, OC12, OC48, OC192 STS1, STS3C, STS12C, STS48C, or STS192C VT1 VCG T1, E1
Description	manual switch
Likely Cause	User selected **Fault** → **Protection Switch** and highlighted an OCN line protection group, RPR protection group, or Path protection group, and provisioned the Switch Type as **Manual**. User selected **Fault** → **Timing/Sync Protection Switch** → **System Timing Reference/Source Switch** and the Switch Command **Manual**. The synchronization reference protection switching has been provisioned to revertive.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-95: “Clear "manual switch" condition” (p. 5-247).

Manual Switch

Description

The protection tributaries (in the specified direction [East or West] on the 2-fiber BLSR) are selected, provided they are good and there are no existing higher priority protection switching requests.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OC-48 line OC-192 line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	MSR (Manual switch)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	OC48 OC192
Description	Manual Switch
Likely Cause	User executed a manual switch on the 2-fiber BLSR using **Fault** → **Protection Switch** and selected Manual To Protection, Ring.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-96: “Clear "Manual Switch" condition” (p. 5-249).

manual sync. mode switch

Description

System timing has been forced to holdover.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Shelf Subshelf
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	HLDOVRSYNC (Holdover synchronization mode)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	manual sync. mode switch
Likely Cause	User selected **Fault** → **Timing/Sync Protection Switch** → **Clock Mode Switch** and the Switch Command **Holdover**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-97: “Clear "manual sync. mode switch" condition” (p. 5-250).

Member Not Collecting/Distributing

Description

The specified LAN port is not collecting (receiving) or distributing (transmitting) packets within the IEEE Std 802.3™-2002 compliant Link Aggregation Group.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	Fast Ethernet port Gigabit Ethernet port
AID Type	Ethernet port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	MNCD (Member Not Collecting/Distributing)
Effect on Service	SA
Alarm Entity Type	FELAN GELAN
Description	Member Not Collecting/Distributing
Likely Cause	The LAN port is not collecting (receiving) or distributing (transmitting) packets due to a configuration conflict with the interfacing customer LAN port (LAG partner). The Link Aggregation Group and/or LAN port provisioning at the interfacing customer equipment is incompatible.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-98: “Clear "Member Not Collecting/ Distributing" alarm” (p. 5-251).

Member Signal Unacceptable - LCAS

Description

A tributary that is provisioned to be a member of a VCG with LCAS enabled is determined to be failed as a result of Loss of Multiframe or its delay is outside the range of differential delay accommodation for the VCG. (SONET failures, for example AIS, mask the `Member Signal Unacceptable – LCAS` alarm.) In response to this alarm, LCAS may remove the tributary from service. If it does, and at least one tributary remains in service, a `VCG Loss of Partial Capacity` alarm is also generated.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Minor (MN) NSA Default: Minor (MN)
ASAP Type	VCG STS Tributary VCG VT1.5 Tributary
AID Type	STS-1 Ring Channel STS-3c Ring Channel VT1.5 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	MSU-L (Member Signal Unacceptable - LCAS)
Effect on Service	SA or NSA
Alarm Entity Type	STS1 STS3C VT1.5
Description	Member Signal Unacceptable - LCAS
Likely Cause	Loss of Multiframe is detected on the STS-1, STS-3c, or VT1.5 tributary that is a member of an LCAS-enabled VCG or the tributary delay is outside the range of differential delay accommodation for the VCG.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the OLIU circuit pack.
Action	Proceed to Procedure 5-99: “Clear "Member Signal Unacceptable - LCAS" alarm” (p. 5-253).

Multiple Databases

Description

The system has detected multiple valid, but different, databases and cannot select the database to use.

Alarm Data	Value/Meaning
Severity Levels	Minor (MN)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	DATAFLT (Data Integrity Fault)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Multiple Databases
Likely Cause	A new nonvolatile memory (NVM) module was installed with a valid database different from the old database, and the system cannot select the database to use.
Visible Indication	Lighted **MN** LED on the SYSCTL faceplate
Action	Proceed to Procedure 5-44: “Clear "Generic/Database/Equipment Configuration" alarms/conditions” (p. 5-104).

Multiple Generics

Description

The system has detected multiple valid, but different, generics and cannot select the generic to use.

Alarm Data	Value/Meaning
Severity Levels	Minor (MN)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	DATAFLT (Data Integrity Fault)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Multiple Generics
Likely Cause	A new nonvolatile memory (NVM) module was installed with a valid generic different from the old generic, and the system cannot select the generic to use.
Visible Indication	Lighted **MN** LED on the SYSCTL faceplate
Action	Proceed to Procedure 5-44: “Clear "Generic/Database/Equipment Configuration" alarms/conditions” (p. 5-104).

Multiple Main Shelf TIDs

Description

During the discovery phase of the communication link establishment procedure, a subshelf in a multi-shelf DCS system received multiple offer packets from different main shelves. The `Multiple Main Shelf TIDs` alarm is only reported in the maintenance mode.

Alarm Data	Value/Meaning
Severity Levels	Minor (MN)
AID Type	Subshelf
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	DATAFLT (Data Integrity Fault)
Effect on Service	NSA
Alarm Entity Type	EQPT
Description	Multiple Main Shelf TIDs
Likely Cause	More than one main shelf, with the same TID, is connected to LAN3, identified as DLAN on the back of a shelf. LAN3 serves as the control communications link between the main shelf and each subshelf.
Visible Indication	Lighted **MN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-135: "Clear "Subshelf-related" alarms/conditions" (p. 5-329).

Muxponder CP failed

Description

An internal equipment failure of the specified Muxponder circuit pack, or a communications problem between the specified circuit pack and the SYSCTL circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA
Alarm Entity Type	EQPT
Description	Muxponder CP failed
Likely Cause	A Muxponder circuit pack failed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the failed circuit pack.
Action	Proceed to Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44).

neighbor SYSCTL CP unavailable (nbr tid = TID)

Description

Neighbor SYSCTL circuit pack is unavailable and/or unable to communicate with the local network element. While this alarm is present, some types of failures at the neighboring node cannot be reported.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	OCn Port
AID Type	OC-3 line OC-12 line OC-48 line OC-192 line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	CONTR (Control processor failure)
Effect on Service	NSA
Alarm Entity Type	OC3 OC12 OC48 OC192
Description	neighbor SYSCTL CP unavailable (nbr tid = *TID*)
Likely Cause	`Section DCC channel failed` alarm present and persisting for five minutes or more, possibly indicating an internal equipment failure on the identified neighbor SYSCTL circuit pack.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-100: “Clear "neighbor SYSCTL CP unavailable (nbr tid = TID)" alarm” (p. 5-257).

Node ID Mismatch

Description

The Node ID Mismatch alarm is generated at nodes in a BLSR when:

- The received Source Node ID does not match an entry in the node's BLSR ring map.
- The Destination Node ID is equal to the node's own Node ID and the Source Node ID is not an adjacent node according to the node's BLSR ring map.
- The received Destination Node ID in a short path message is not equal to the node's own Node ID or the Source Node ID is not an adjacent node according to the node's BLSR ring map.
- The Destination Node ID is equal to the node's own Node ID and the Source Node ID is not an adjacent node according to the node's BLSR ring map.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	BLSR Protection Group
AID Type	OC-48 line OC-192 line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	NID-CONFL (Node ID conflict)
Effect on Service	NSA
Alarm Entity Type	OC48 OC192
Description	Node ID Mismatch
Likely Cause	The BLSR manual ring map was not provisioned correctly.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-101: “Clear "Node ID Mismatch" alarm” (p. 5-260).

NP audit failed

Description

Transmission audits are enabled on the circuit pack and the system has detected a network processor audit failure.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	NPAUDT (NP audit failed)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	NP audit failed
Likely Cause	A failed device on the circuit pack caused a packet flow problem, or there are excessive broadcast type Ethernet frames running through the network processor. The maximum through capacity is 9 Gigabits.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-4: “Clear "audit failed" alarms” (p. 5-21).

NSAP count in L1 overflowed

Description

The NSAP count for the level 1 routing area has exceeded 250 nodes.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	System
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	BUFROVLD (Buffer overload)
Effect on Service	NSA
Alarm Entity Type	COM
Description	NSAP count in L1 overflowed
Likely Cause	The number of OSI nodes in the level 1 routing area has exceeded 250.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-102: “Clear "NSAP count in L1 overflowed" alarm” (p. 5-264).

NSAP count in L1 threshold crossed

Description

The NSAP count for the level 1 routing area has exceeded the provisioned threshold.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	System
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	BUFROVLD (Buffer overload)
Effect on Service	NSA
Alarm Entity Type	COM
Description	NSAP count in L1 threshold crossed
Likely Cause	The number of OSI nodes in the level 1 routing area has exceeded the provisioned threshold.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-103: “Clear "NSAP count in L1 threshold crossed" alarm” (p. 5-265).

NTP server(s) unreachable

Description

The network element is provisioned for network time protocol (NTP), and the network element cannot communicate with any NTP server.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC (EOC failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	NTP server(s) unreachable
Likely Cause	Incorrect provisioning of the NTP feature, LAN, or network failures.
Visible Indication	None
Action	Proceed to Procedure 5-104: “Clear "NTP server(s) unreachable" condition” (p. 5-266).

NUT Inconsistent XC Granularity

Description

Operational NUT on the indicated cross-connection is inconsistent across all tributaries on the cross-connection. For example, in an STS-3c cross-connection, the three tributaries do not share a consistent protection behavior; Tributary 1 and 2 are PROT and Tributary 3 is NOTPR.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	BLSR Protection Group
AID Type	STS-n Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	NUTINXCGRN (NUT inconsistent cross connect granularity)
Effect on Service	NSA
Alarm Entity Type	COM
Description	NUT Inconsistent XC Granularity
Likely Cause	Local NUT was provisioned at a remote node in the BLSR which results in inconsistent operational NUT on an existing cross-connection at the local node.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-105: “Clear "NUT Inconsistent XC Granularity" alarm” (p. 5-267).

NVM failed

Description

An internal equipment failure of the specified nonvolatile memory (NVM) module, or a communications problem between the NVM module and the SYSCTL circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN) Default: Critical (CR)
ASAP Type	Non-Volatile Memory Module
AID Type	NVM
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	WKGMEM (Working Memory Failure)
Effect on Service	NSA
Alarm Entity Type	EQPT
Description	NVM failed
Likely Cause	The NVM module failed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the circuit pack. The **IND** display shows *N0x* where *x* is the failed NVM number.
Action	Proceed to Procedure 5-106: “Clear "NVM" alarms” (p. 5-269).

NVM removed or NVM failed

Description

An NVM module is missing, or an internal equipment failure occurred on the specified NVM module.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN) Default: Critical (CR)
ASAP Type	Non-Volatile Memory Module
AID Type	NVM
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	WKGMEM (Working Memory Failure)
Effect on Service	NSA
Alarm Entity Type	EQPT
Description	NVM removed or NVM failed
Likely Cause	The NVM module is either failed or missing from the SYSCTL circuit pack.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the circuit pack. The **IND** display shows *N0x* where *x* is the missing/failed NVM number.
Action	Proceed to Procedure 5-106: "Clear "NVM" alarms" (p. 5-269).

NVM write disabled

Description

An NVM module has either failed or was removed, and the system has entered the NVM write disabled state to protect the database and maintain transmission.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	NVM
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	WKGMEM (Working Memory Failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	EQPT
Description	NVM write disabled
Likely Cause	An NVM module has either failed or was removed.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	No action is necessary. The Standing Condition clears when all NVM-related alarms are cleared.

OCN facility loopback

Description

A facility loopback is active on the specified OCN port.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OCN Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	High Speed (main): OC12, OC48, OC192 Low Speed (function): OC3, OC12, OC48
Description	OCN facility loopback
Likely Cause	User executed a facility loopback using **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-107: “Clear "OCN facility loopback" condition” (p. 5-274).

OCN terminal loopback

Description

A terminal loopback is active on the specified OCN port.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OCN Line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	LPBKNETWORK (Loopback, Network)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	Low Speed (function): OC3, OC12, OC48
Description	OCN terminal loopback
Likely Cause	User executed a terminal loopback using **Fault** → **Analysis** → **Loopback**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-108: “Clear "OCN terminal loopback" condition” (p. 5-275).

OLIU CP failed

Description

An internal equipment failure of the specified OC-3/OC-12/OC-48/OC-192 OLIU circuit pack, or a communications problem between the specified circuit pack and the SYSCTL circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	OLIU CP failed
Likely Cause	An unprotected OLIU circuit pack carrying service failed - SA. A protected OLIU circuit pack failed - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the failed circuit pack.
Action	Proceed to Procedure 5-13: "Clear "CP failed/CP contributing to a pack failure" alarms" (p. 5-44).

OMD CP failed

Description

An internal equipment failure of the specified OMD circuit pack, or a communications problem between the specified circuit pack and the SYSCTL circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA
Alarm Entity Type	EQPT
Description	OMD CP failed
Likely Cause	An OMD circuit pack failed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the failed circuit pack.
Action	Proceed to Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44).

Path Integrity Failure

Description

There is discontinuity in the circuit path.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	BLSR Protection Group
AID Type	STS-n Ring Channel VT1.5 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	PAINTGRT (Path Integrity)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Path Integrity Failure
Likely Cause	Cross-connect provisioning error (for example, missing pass-through) at some point in the circuit.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-112: “Clear "Path Integrity Failure" alarm” (p. 5-281).

Pluggable Transmission Module insufficient maximum rate

Description

The XFP pluggable transmission module installed in the specified socket does not support the port rate.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Pluggable Transmission Module
AID Type	Socket
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	Pluggable Transmission Module insufficient maximum rate
Likely Cause	An unprotected XFP pluggable transmission module that does not support the port rate was installed in the circuit pack- SA. A protected XFP pluggable transmission module that does not support the port rate was installed in the circuit pack - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively), a continuously lighted **Fault** LED on the pluggable transmission module socket, and a flashing **Fault** LED on the circuit pack.
Action	Proceed to Procedure 5-109: “Clear "Pluggable Transmission Module insufficient maximum rate" alarm” (p. 5-276).

Pluggable Transmission Module maintenance IP

Description

The Maintenance State parameter of the specified socket is provisioned to *Maint*.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Pluggable Transmission Module
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	MAN (Manually caused abnormal condition)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	EQPT
Description	Pluggable Transmission Module maintenance IP
Likely Cause	User provisioned the socket Maintenance State parameter to *Maint*.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate. When this standing condition is present, if the pluggable transmission module is removed from the socket, the severity level is at the highest NA, regardless of the provisioned ASAP severity level.
Action	Proceed to Procedure 5-110: “Clear "Pluggable Transmission Module maintenance IP" condition” (p. 5-278).

Pluggable Transmission Module removed

Description

Specified Pluggable Transmission Module was removed from the circuit pack.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Pluggable Transmission Module
AID Type	Socket
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	Pluggable Transmission Module removed
Likely Cause	An unprotected pluggable transmission module was removed from the circuit pack- SA. A protected pluggable transmission module was removed from the circuit pack - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively), a continuously lighted **Fault** LED on the empty pluggable transmission module socket, and a flashing **Fault** LED on the circuit pack.
Action	Proceed to Procedure 5-111: “Clear "Pluggable Transmission Module removed" alarm” (p. 5-279).

Port administratively disabled

Description

The Port Administration Control parameter is disabled. All frames to and from the port are disabled.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Data port Ethernet port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	MAN (Manually caused abnormal condition)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	DATA FELAN GELAN
Description	Port administratively disabled
Likely Cause	User disabled the Port Administration Control parameter using **Configuration** → **Equipment**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-113: “Clear "Port administratively disabled" condition” (p. 5-282).

Protection CP Input fault

Description

A loss of signal or loss of frame defect has been detected on the protection circuit pack but not on the corresponding active circuit pack.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	NSA
Alarm Entity Type	EQPT
Description	Protection CP Input fault
Likely Cause	Incoming loss of signal, incoming loss of frame defect, or local circuit pack failure.
Visible Indication	A flashing **Fault** LED on the alarmed circuit pack. Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-116: “Clear "PROTN Port Failure/Protection CP Input fault" alarms” (p. 5-287).

Protection switching byte failure

Description

The near-end network element is receiving unstable K-bytes in the APS channel for the 1+1_BIDIR or 1+1_OPTM protection group (bits 5–8 of the K1 byte), or the near-end network element is receiving K-bytes with invalid values. The APS channel is provided by the K1 and the K2 bytes in the SONET section overhead of an OC-N to communicate the protection switching protocol between the local and far-end nodes.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP type	1+1 Bidirectional Protection Group 1+1 Optimized Protection Group
AID Type	OC-N line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	APSB (APS Byte Failure)
Effect on Service	NSA
Alarm Entity Type	OCN
Description	Protection switching byte failure
Likely Cause	The OC-N line at the near-end network element has been provisioned to 1+1_BIDIR or 1+1_OPTM, but the OC-N line at the far-end network element has been provisioned to an incompatible protection group type. For example, the near-end OC-N line is provisioned to 1+1_BIDIR, and the far-end OC-N line is *not* provisioned to 1+1_BIDIR.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-114: “Clear "Protection switching byte failure" alarm” (p. 5-283).

Protection switching channel match failure

Description

The near-end network element is receiving an unexpected channel number in the K-bytes in the APS channel (bits 1–4 of the K2 byte) for the 1+1_BIDIR or 1+1_OPTM protection group. The APS channel is provided by the K1 and the K2 bytes in the SONET section overhead of an OC-N to communicate the protection switching protocol between the local and far-end nodes.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	1+1 Bidirectional Protection Group 1+1 Optimized Protection Group
AID Type	OC-N line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	APSCM (APS Channel Match Failure)
Effect on Service	NSA
Alarm Entity Type	OCN
Description	Protection switching channel match failure
Likely Cause	The OC-N line at the near-end network element has been provisioned to 1+1_BIDIR or 1+1_OPTM, but the OC-N line at the far-end network element has been provisioned to an incompatible protection group type. For example, the near-end OC-N line is provisioned to 1+1_BIDIR, and the far-end OC-N line is *not* provisioned to 1+1_BIDIR.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-115: “Clear "Protection switching channel match failure" alarm” (p. 5-285).

PROTN DS3 Port Failure

Description

A loss of signal or loss of frame defect has been detected on a protection DS3 port but not on the corresponding active DS3 port.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	DS3 Port
AID Type	DS3 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	PROTN (Protection unit not available)
Effect on Service	NSA
Alarm Entity Type	T3
Description	PROTN DS3 Port Failure
Likely Cause	Incoming loss of signal, incoming loss of frame defect, or local circuit pack failure.
Visible Indication	A flashing **Fault** LED on the alarmed circuit pack. Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-116: “Clear "PROTN Port Failure/Protection CP Input fault" alarms” (p. 5-287).

PROTN EC1 Port Failure

Description

A loss of signal or loss of frame defect has been detected on a protection EC-1 port but not on the corresponding active EC-1 port.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	EC1 Port
AID Type	EC-1 Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	PROTN (Protection unit not available)
Effect on Service	NSA
Alarm Entity Type	EC1
Description	PROTN EC1 Port Failure
Likely Cause	Incoming loss of signal, incoming loss of frame defect, or local circuit pack failure.
Visible Indication	A flashing **Fault** LED on the alarmed circuit pack. Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-116: “Clear "PROTN Port Failure/Protection CP Input fault" alarms” (p. 5-287).

Receive buffer overflow

Description

The Data port is provisioned for synchronous FC, FICON, or ESCON operation and the SONET bandwidth is not full rate.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Data port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	BUFROVLD (Buffer overload)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	DATA
Description	Receive buffer overflow
Likely Cause	Insufficient SONET bandwidth (not full rate).
Visible Indication	None
Action	Proceed to Procedure 5-117: “Clear "Receive buffer overflow" condition” (p. 5-290).

Remote client signal failed

Description

Indicates that the far-end equipment has detected an incoming client signal failure.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	VCG Port
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	GFP_RCF (Remote Client Fail)
Effect on Service	SA
Alarm Entity Type	VCG
Description	Remote client signal failed
Likely Cause	Incoming client signal failure detected at the far-end equipment.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-118: “Clear "Remote client signal failed" alarm” (p. 5-292).

remote install/copy program IP

Description

The system is receiving a software generic into the dormant area from a remote network element.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC (EOC failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	remote install/copy program IP
Likely Cause	User selected **Configuration** → **Software** → **Copy Software** from the remote network element.
Visible Indication	None
Action	No action is necessary. The condition clears automatically when the generic is completely copied into the dormant area of the network element.

Ring Circuit Alarm Suppressed

Description

The ring circuit alarm reporting is disabled on the local node.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	BLSR protection group
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	CKTAUDUD (Circuit Audit Suppressed)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	Ring Circuit Alarm Suppressed
Likely Cause	User selected **Configuration** → **Equipment**, selected the **Ptn Grp**, selected a 2F BLSR protection group and provisioned the Ring Circuit Alarm Mode to **Disabled.**
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-119: “Clear "Ring Circuit Alarm Suppressed" condition” (p. 5-295)

Ring Ckt Validation Suspended

Description

During automatic ring discovery (ARD), validation of the ring's circuits is suspended until all nodes in the ring have the cross-connect maps for all other nodes in the ring.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	BLSR Protection Group
AID Type	BLSR protection group
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	CKTAUDSNP (Circuit Audit Suspended)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Ring Ckt Validation Suspended
Likely Cause	The cross-connect maps have not been distributed across the ring.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-120: “Clear "Ring Ckt Validation Suspended" alarm” (p. 5-296)

Ring Comm Failure

Description

The during automatic ring discovery, the ring map could not be completed because of a DCC communications failure.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (Mn)
ASAP Type	BLSR Protection Group
AID Type	BLSR protection group
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RNG-DSCVY (Ring Discovery)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Ring Comm Failure
Likely Cause	During auto discovery, the ring map could not be completed because of a DCC communication failure.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-121: “Clear "Ring Comm Failure" alarm” (p. 5-298).

Ring Discovery In Progress

Description

The system is in the process of searching for a provisioned BLSR or searching for neighbors or nodes newly added to an existing ring map.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	BLSR protection group
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RNG-DSCVY (Ring Discovery)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	Ring Discovery In Progress
Likely Cause	Alcatel-Lucent 1665 DMX has been added to a ring and the system is searching for the existing ring map.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	No action is necessary. Wait for Automatic Ring Discovery to complete a valid ring map.

Ring Incomplete

Description

During BLSR automatic ring discovery, the ring map could not be completed. The network element tries continuously, at 1-minute intervals, to establish a correct ring topology.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	BLSR Protection Group
AID Type	BLSR protection group
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RNG-INC (Ring Incomplete)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Ring Incomplete
Likely Cause	Manual ring map provisioning was not applied or was the ring map was not provisioned correctly. During BLSR auto ring discovery, the ring map could not be completed, because • no OSI association to the neighboring nodes. • no LinkID or LinkID mismatch.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-122: “Clear "Ring Incomplete" alarm” (p. 5-301).

Ring Prot Switching Suspended

Description

BLSR protection switching is temporarily suspended because a valid ring map does not exist or a node does not have a Node ID.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	BLSR Protection Group
AID Type	BLSR protection group
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	OVRDSW (Override Switch)
Effect on Service	NSA
Alarm Entity Type	OC48 OC192
Description	Ring Prot Switching Suspended
Likely Cause	A new node is introduced to the BLSR and does not have a ring map, or the ring map is invalid; BLSR protection switching is disabled.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-123: “Clear "Ring Prot Switching Suspended" alarm” (p. 5-307).

ring upgrade mode

Description

The network element is in the provisioned ring upgrade mode.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RINGUPGRADE
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	ring upgrade mode
Likely Cause	User selected **Configuration** → **Ring Upgrade Mode**. This command is used in network upgrades.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-124: “Clear "ring upgrade mode" condition” (p. 5-309).

RPR Miscabling

Description

The West side of the node (VCG v1) is connected to the West side of the adjacent node (VCG v1), or the East side of the node (VCG v2) is connected to the East side of the adjacent node (VCG v2).

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	MISCBL (RPR Miscabling)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	VCG
Description	RPR Miscabling
Likely Cause	VCG v1 at the local node was cross-connected so that it is connected to VCG v1 at the adjacent node, or VCG v2 at the local node was cross-connected so that it is connected to VCG v2 at the adjacent node. (VCG v1 must be connected to VCG v2 between adjacent nodes.)
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-125: “Clear "RPR Miscabling" condition” (p. 5-310).

RPR Topology Exceeded Max Stations

Description

The number of nodes in the ring has exceeded 255. RPR rings support a maximum of 255 nodes.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	TOPO-MAX (RPR - Topology Exceeded Max Stations)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	VCG
Description	RPR Topology Exceeded Max Stations
Likely Cause	The number of nodes in the ring has exceeded the maximum of 255.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-126: “Clear "RPR Topology Exceeded Max Stations" condition” (p. 5-312).

RPR Topology Inconsistency

Description

A duplicate RPR MAC address or a ring misconfiguration exists that is causing the ring map to appear different between ringlet 0 and ringlet 1.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	TOPO-INCS (RPR - Topology Inconsistency)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	VCG
Description	RPR Topology Inconsistency
Likely Cause	A duplicate RPR MAC address exists in the ring or a ring span is not connected bidirectionally to an adjacent node.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-127: “Clear "RPR Topology Inconsistency" condition” (p. 5-313).

RPR Topology Map Entry Invalid

Description

The provisionable VCG Topology Stability Timer does not allow enough time for the ring to stabilize after a topology change.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	TOPO-INV (RPR - Topology Map Entry Invalid)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	VCG
Description	RPR Topology Map Entry Invalid
Likely Cause	The provisionable VCG *Topology Stability Timer* is too short for the ring to stabilize after a topology change.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-128: “Clear "RPR Topology Map Entry Invalid" condition” (p. 5-315).

RPR Topology Unstable

Description

Multiple or repetitive RPR topology changes (for example, protection switches) occurred whose duration exceeded the provisionable VCG Topology Stability Timer.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	TOPO-UNST (RPR - Topology Unstable)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	VCG
Description	RPR Topology Unstable
Likely Cause	Multiple or repetitive RPR topology changes occurred whose duration exceeded the provisionable VCG *Topology Stability Timer*. RPR Topology changes include protection switches and adding/deleting nodes to/from the ring.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-129: “Clear "RPR Topology Unstable" condition” (p. 5-316).

section DCC channel failed

Description

The system cannot communicate with the far-end system through the SONET section data communications channel (DCC).

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	OCn Port
AID Type	Section Data Communications Channel (DCC)
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC (EOC failure)
Effect on Service	NSA
Alarm Entity Type	COM
Description	section DCC channel failed
Likely Cause	SYSCTL circuit pack failed, reset, or initialized at the far-end The program installation failed at the far-end The program installation is in progress at the far-end The OC-N OLIU circuit pack failed at the near-end
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-130: “Clear "section DCC channel failed" alarm” (p. 5-317).

Segment audit failed LAN in

Description

Transmission audits are enabled on the circuit pack and the system has detected a segment audit failure on the specified incoming LAN.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	Circuit pack Fast Ethernet port Gigabit Ethernet port
AID Type	Slot Ethernet 10/100T Port Ethernet 1GbE Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SEGAUDTIN (Segment audit failed in)
Effect on Service	SA
Alarm Entity Type	EQPT FELAN GELAN
Description	Segment audit failed LAN in
Likely Cause	A failed device on the circuit pack caused a packet flow problem on the specified incoming LAN.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-4: “Clear "audit failed" alarms” (p. 5-21).

Segment audit failed LAN out

Description

Transmission audits are enabled on the circuit pack and the system has detected a segment audit failure on the specified outgoing LAN.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Critical (CR)
ASAP Type	Circuit pack Fast Ethernet port Gigabit Ethernet port
AID Type	Slot Ethernet 10/100T Port Ethernet 1GbE Port
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SEGAUDTOUT (Segment audit failed out)
Effect on Service	SA
Alarm Entity Type	EQPT FELAN GELAN
Description	Segment audit failed LAN out
Likely Cause	A failed device on the circuit pack caused a packet flow problem on the specified outgoing LAN.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-4: “Clear "audit failed" alarms” (p. 5-21).

Segment audit failed VCG in

Description

Transmission audits are enabled on the circuit pack and the system has detected a segment audit failure on the specified incoming VCG.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	VCG port
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SEGAUDTIN (Segment audit failed in)
Effect on Service	SA or NSA
Alarm Entity Type	VCG
Description	Segment audit failed VCG in
Likely Cause	A failed device on the circuit pack caused a packet flow problem on the specified incoming VCG.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-4: “Clear "audit failed" alarms” (p. 5-21).

Segment audit failed VCG out

Description

Transmission audits are enabled on the circuit pack and the system has detected a segment audit failure on the specified outgoing VCG.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	VCG port
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SEGAUDTOUT (Segment audit failed out)
Effect on Service	SA or NSA
Alarm Entity Type	VCG
Description	Segment audit failed VCG out
Likely Cause	A failed device on the circuit pack caused a packet flow problem on the specified outgoing VCG.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-4: “Clear "audit failed" alarms” (p. 5-21).

Squelch Map Inconsistent

Description

Provisioned source and destination (loca/locz) value does not match other provisioned loca/locz values on other cross-connects that are part of circuit.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	BLSR Protection Group
AID Type	STS-n Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SQMAP-INCST (Squelch Map Inconsistent)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Squelch Map Inconsistent
Likely Cause	User selected **Configuration** → **Equipment**, selected the Ptn Grp, selected a 2F BLSR protection group and provisioned the Auto Squelch Map to Manual and incorrectly provisioned the loca/locz parameters on one or more cross-connections in the circuit.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-131: “Clear "Squelch Map Inconsistent" alarm” (p. 5-321).

Squelch Data Unavailable

Description

The network element could not find the source and/or destination ID for the specified cross-connections in the circuit.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	BLSR Protection Group
AID Type	STS-n Ring Channel VT Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	SQDATA-UNAV (Squelch Map Unavailable)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Squelch Data Unavailable
Likely Cause	User selected **Configuration** → **Equipment**, selected the Ptn Grp, selected a 2F BLSR protection group and provisioned the Auto Squelch Map to Auto. All cross-connects in the circuit are not provisioned. Therefore, the network element cannot complete the squelch map.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-132: “Clear "Squelch Data Unavailable" alarm” (p. 5-322).

STP autolock port disable

Description

The number of STP port state changes has exceeded the provisioned threshold for the specified Ethernet port, VCG, or link aggregation group and the port is disabled.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	Fast Ethernet port Gigabit Ethernet port VCG port Link Aggregation Group
AID Type	Ethernet 10/100T port Ethernet GbE port LAG VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	AUTOLOCK (Auto Lock port in spanning tree group)
Effect on Service	SA
Alarm Entity Type	FELAN GELAN LAG VCG
Description	STP autolock port disable
Likely Cause	The STP state is unstable and rapidly reconfiguring. The number of STP state changes has exceeded the provisioned threshold.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a flashing **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-133: “Clear "STP autolock port disable" alarm” (p. 5-324).

Subshelf Boot Failed

Description

During the subshelf startup procedure, a subshelf communication failure occurred, a software download failed, or a database download failed. The `Subshelf Boot Failed` alarm is only reported in the maintenance mode.

Alarm Data	Value/Meaning
Severity Levels	Minor (MN)
AID Type	Subshelf
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	DATAFLT (Data Integrity Fault)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Subshelf Boot Failed
Likely Cause	A subshelf communication failure, software download failure, or database download failure occurred.
Visible Indication	Lighted **MN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-135: "Clear "Subshelf-related" alarms/conditions" (p. 5-329).

Subshelf Communication Failed

Description

The main shelf or a subshelf in a multishelf DCS system has failed to receive at least one valid inter-shelf communication message in any 60 +/-5 second interval.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Major (MJ)
ASAP Type	Subshelf
AID Type	Subshelf
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	REMLINK (Host/Remote Subsystem Link Failure)
Effect on Service	CR, MJ, MN = NSA Not Alarmed = Standing Condition (SC)
Alarm Entity Type	EQPT
Description	Subshelf Communication Failed
Likely Cause	The LAN3 connection, identified as DLAN on the back of a shelf, or the control communications link between the main shelf and each subshelf failed. To support more than one subshelf, the LAN3 port of the main shelf and of each subshelf must be connected to an Ethernet hub capable of supporting 100Mb operation. No special cable is required.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, Minor, or Not Alarmed respectively).
Action	Proceed to Procedure 5-134: “Clear "Subshelf Communication Failed” alarm” (p. 5-326).

Subshelf Configuration Mismatch

Description

During the subshelf startup procedure, a subshelf detected the local subshelf information (subshelf MAC address and ssconfig.dat file) does not match the subshelf information provisioned on the main shelf. The `Subshelf Configuration Mismatch` alarm is only reported in the maintenance mode.

Alarm Data	Value/Meaning
Severity Levels	Minor (MN)
AID Type	Subshelf
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	DATAFLT (Data Integrity Fault)
Effect on Service	NSA
Alarm Entity Type	COM
Description	Subshelf Configuration Mismatch
Likely Cause	The local subshelf information (subshelf MAC address and ssconfig.dat file) does not match the subshelf information provisioned on the main shelf.
Visible Indication	Lighted **MN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-135: “Clear "Subshelf-related" alarms/conditions” (p. 5-329).

Subshelf initialization IP

Description

A subshelf in a multishelf DCS system is initializing. The main shelf reports the `Subshelf Initialization IP` alarm.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Not Alarmed (NA)
ASAP Type	Subshelf
AID Type	Subshelf
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC (EOC Failure)
Effect on Service	CR, MJ, MN = NSA Not Alarmed = Standing Condition (SC)
Alarm Entity Type	EQPT
Description	Subshelf initialization IP
Likely Cause	A new subshelf is being installed.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, Minor, or Not Alarmed respectively).
Action	No action is necessary. The condition clears automatically after the affected subshelf initializes.

SYSCTL CP failed

Description

An internal equipment failure of the SYSCTL circuit pack. While this alarm is present, some types of failures cannot be reported because the SYSCTL circuit pack cannot function under these conditions.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	CONTR (Control processor failure)
Effect on Service	NSA
Alarm Entity Type	EQPT
Description	SYSCTL CP failed
Likely Cause	Internal equipment failure of the SYSCTL circuit pack.
Visible Indication	None or lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively).
Action	Proceed to Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44).

SYS dorm area corrupted

Description

The dormant generic is corrupt or missing.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC (EOC failure)
Effect on Service	Standing Condition
Alarm Entity Type	COM
Description	SYS dorm area corrupted
Likely Cause	The dormant version of the generic is corrupted.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-136: “Clear "SYS dorm area corrupted" condition” (p. 5-339).

SYS generic corrupted

Description

The system has detected a corrupted generic during a software apply operation.

Alarm Data	Value/Meaning
Severity Levels	Major (MJ)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	EOC (EOC failure)
Effect on Service	NSA
Alarm Entity Type	COM
Description	SYS generic corrupted
Likely Cause	The current version of the generic is corrupted.
Visible Indication	Lighted **MJ** LED on the SYSCTL faceplate
Action	Proceed to Procedure 5-137: "Clear "SYS generic corrupted" alarm" (p. 5-340).

SWITCH CP failed

Description

An internal equipment failure of the specified LNW80 SWITCH circuit pack, or a communications problem between the specified circuit pack and the SYSCTL circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	NSA
Alarm Entity Type	EQPT
Description	SWITCH CP failed
Likely Cause	Internal equipment failure of the SWITCH circuit pack.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the failed circuit pack.
Action	Proceed to Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44).

Temporarily NUT Provisioned

Description

A node in the BLSR in a local NUT configuration has a timeslot set to Temp Not Protected.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	STS-n Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	NUTTMPPRV (Temporarily NUT Provisioned)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	Temporarily NUT provisioned
Likely Cause	User selected **Configuration** → **Equipment**, selected a 2F BLSR protection group and provisioned the NUT feature.
Visible Indication	None
Action	Proceed to Procedure 5-138: “Clear "Temporarily NUT Provisioned" condition” (p. 5-342).

Test access IP

Description

A test access session is in progress on the specified channel.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	STS-1 Ring Channel, VT1.5 Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	TSTACC (Test Access)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	STS1 VT1
Description	Test access IP
Likely Cause	User selected **Fault** → **Analysis** → **Test Access**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-139: “Clear "Test access IP" conditions” (p. 5-343).

Test access IP:*tsn*

Description

A test access session, identified by the test session number (tsn), is in progress.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	STS-1 or STS-3c Ring Channel
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	TSTACC (Test Access)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	STS1 STS3c
Description	Test access IP:*tsn*
Likely Cause	User selected **Fault** → **Analysis** → **Test Access**.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-139: “Clear "Test access IP" conditions” (p. 5-343).

time of day not provisioned

Description

The network element time of day is not provisioned.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Blank
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	CONTR (Control processor failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	time of day not provisioned
Likely Cause	The SYSCTL circuit pack has been reset.
Visible Indication	None
Action	Proceed to Procedure 5-140: “Clear "time of day not provisioned" condition” (p. 5-344).

TMUX CP failed

Description

An internal equipment failure of the specified TMUX circuit pack, or a communication problem between the specified TMUX circuit pack and the SYSCTL circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	TMUX CP failed
Likely Cause	An unprotected TMUX circuit pack (LNW18 or LNW20) failed - SA. A protected TMUX circuit pack failed - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the failed circuit pack.
Action	Proceed to Procedure 5-13: “Clear "CP failed/CP contributing to a pack failure" alarms” (p. 5-44).

Traffic Squelched

Description

Multiple failures have isolated a node or nodes in a BLSR. At switching nodes, an alarm indication signal (AIS) is inserted on any traffic coming to/from an isolated node(s) to protect against improperly connecting traffic. Extra traffic, if supported, is squelched at the drop nodes.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	OC-48 line OC-192 line
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RNG-SQUELCH (Traffic Squelched on Ring)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	OC48 OC192
Description	Traffic Squelched
Likely Cause	Ring segmentation due to multiple failures in the BLSR; inc. OC-48/OC-192 line AIS, inc. OC-48/OC-192 LOS, or inc. OC-48/OC-192 LOF alarms are detected at two nodes on the BLSR; node power failure occurred at another node in the BLSR; simultaneous forced switches on different spans in the BLSR.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-141: “Clear "Traffic Squelched" condition” (p. 5-346).

unexpected circuit pack type

Description

The network element is in the provisioned Ring Upgrade mode and a different but compatible circuit pack is inserted into a slot that is provisioned for another circuit pack type.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	EQPT
Description	unexpected circuit pack type
Likely Cause	An unexpected compatible circuit pack is in a slot as part of a node or network upgrade.
Visible Indication	A continuously lighted **Fault** LED on the affected circuit pack.
Action	No action is necessary. The Standing Condition will clear when the upgrade is complete.

unexpected CP type

Description

This alarm indicates that a different but supported circuit pack is inserted into a slot that is provisioned for another circuit pack type.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	unexpected CP type
Likely Cause	The wrong circuit pack was inserted into an unprotected slot. - SA. The wrong circuit pack was inserted into a protected slot - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the affected circuit pack.
Action	Proceed to Procedure 5-142: “Clear "unexpected CP type" alarm” (p. 5-351).

unexpected or failed Pluggable Transmission Module

Description

An internal equipment failure of the specified pluggable transmission module was detected, the wrong pluggable transmission module was inserted into the socket, or a communications problem between the pluggable transmission module and the SYSCTL circuit pack was detected.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Critical (CR) NSA Default: Minor (MN)
ASAP Type	Pluggable Transmission Module
AID Type	Socket
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	unexpected or failed Pluggable Transmission Module
Likely Cause	An unprotected pluggable transmission module failed or the wrong pluggable transmission module was inserted into an unprotected socket - SA. A protected pluggable transmission module failed or the wrong pluggable transmission module was inserted into a protected socket - NSA.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively), a continuously lighted **Fault** LED on the failed pluggable transmission module socket, and a flashing **Fault** LED on the circuit pack.
Action	Proceed to Procedure 5-143: “Clear "unexpected or failed Pluggable Transmission Module" alarm” (p. 5-353).

Unknown Ring Type

Description

Alcatel-Lucent 1665 DMX does not recognize the ring type.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	BLSR protection group
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	RNG-URT (Unknown Ring Type)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	Unknown Ring Type
Likely Cause	Automatic ring discovery did not time out but the ring type could not be determined.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	Proceed to Procedure 5-144: “Clear "Unknown Ring Type" condition” (p. 5-356).

unrecoverable hardware failure during download, replace CP

Description

The affected circuit pack failed when downloading software as part of applying new software to the network element.

Alarm Data	Value/Meaning
Severity Levels	Major (MJ)
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	SA or NSA
Alarm Entity Type	EQPT
Description	unrecoverable hardware failure during download, replace CP
Likely Cause	A non-recoverable circuit pack failure occurred before a successful software download was confirmed.
Visible Indication	Lighted **MJ** LED on the SYSCTL faceplate and a continuously lighted **Fault** LED on the affected circuit pack.
Action	Proceed to Procedure 5-145: “Clear "unrecoverable hardware failure during download, replace CP" alarm” (p. 5-357).

VCG Failure of LCAS Protocol (Sink)

Description

This alarm indicates an LCAS-enabled VCG receive protocol failure.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Minor (MN) NSA Default: Minor (MN)
ASAP Type	VCG Port
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	VCGFOPR (Failure of Protection, Sink)
Effect on Service	SA or NSA
Alarm Entity Type	VCG
Description	VCG Failure of LCAS Protocol (Sink)
Likely Cause	A combination of link failures and provisioning actions are interfering with each other, or a misalignment exists between the source and sink end of the Sequence Numbers and Member Status information.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-146: “Clear "VCG Failure of LCAS Protocol" alarms” (p. 5-359).

VCG Failure of LCAS Protocol (Source)

Description

This alarm indicates an LCAS-enabled VCG transmit protocol failure.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Minor (MN) NSA Default: Minor (MN)
ASAP Type	VCG Port
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	VCGFOPT (Failure of Protection, Source)
Effect on Service	SA or NSA
Alarm Entity Type	VCG
Description	VCG Failure of LCAS Protocol (Source)
Likely Cause	A combination of link failures and provisioning actions that interfered with each other, or a misalignment between the source and sink end of the Sequence Numbers and Member Status information.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-146: “Clear "VCG Failure of LCAS Protocol" alarms” (p. 5-359).

VCG Loss of Partial Capacity

Description

VCG has LCAS enabled, and the number of active members (tributary assigned to a VCG) are automatically reduced due to a failure of either the source (transmit direction) or sink (receive direction), but at least one tributary is still active.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) SA Default: Minor (MN) NSA Default: Minor (MN)
ASAP Type	VCG Port
AID Type	VCG
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	VCGLOPC (Loss of Partial Capacity)
Effect on Service	SA or NSA
Alarm Entity Type	VCG
Description	VCG Loss of Partial Capacity
Likely Cause	A SONET defect (for example, AIS) is detected on the STS-1, STS-3c, or VT1.5 tributary that is also a member of an LCAS-enabled VCG.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively)
Action	Proceed to Procedure 5-147: “Clear "VCG Loss of Partial Capacity" alarm” (p. 5-361).

version mismatch

Description

The firmware in the indicated circuit pack does not match the active software generic running on the network element.

Alarm Data	Value/Meaning
Severity Levels	Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), Not Reported (NR) Default: Minor (MN)
ASAP Type	Circuit pack
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	NSA
Alarm Entity Type	EQPT
Description	version mismatch
Likely Cause	A circuit pack with a newer version of firmware was installed in a shelf and did not update automatically. A new circuit pack was inserted into the shelf, the software generic in the dormant area of the SYSCTL was corrupted or did not match the generic running on the shelf, and the firmware did not update automatically.
Visible Indication	Lighted **CR**, **MJ**, or **MN** LED on the SYSCTL faceplate (when the severity level is provisioned to Critical, Major, or Minor, respectively) and a continuously lighted **Fault** LED on the alarmed circuit pack.
Action	Proceed to Procedure 5-148: “Clear "version mismatch" alarm” (p. 5-365).

waiting for download

Description

The system is the process of upgrading the firmware on more than one circuit pack.

Alarm Data	Value/Meaning
Severity Levels	Not Alarmed (NA)
AID Type	Slot
Date	Month/day/year that the condition was detected
Time	Hour:minute:second that the condition was detected
Probable Cause	FACTERM (Facility termination equipment failure)
Effect on Service	Standing Condition (SC)
Alarm Entity Type	COM
Description	waiting for download
Likely Cause	User selected **Configuration** → **Software** → **Apply Software** and the generic successfully installed in the SYSCTL. The firmware in the smart circuit pack(s) is now upgraded. This condition is present for the circuit packs that are waiting for their firmware to be upgraded.
Visible Indication	Lighted **ABN** LED on the SYSCTL faceplate.
Action	No action is necessary. The condition clears automatically when a circuit pack firmware upgrade is complete.

4 Maintenance overview

Overview

Purpose

This chapter provides an overview of maintenance in the Alcatel-Lucent 1665 Data Multiplexer.

Contents

Introduction

Overview

This chapter defines the maintenance philosophy and describes the features available to monitor and maintain Alcatel-Lucent 1665 Data Multiplexer (Alcatel-Lucent 1665 DMX).

Objectives

This chapter provides information to perform the following

- Define the maintenance philosophy for Alcatel-Lucent 1665 DMX.
- Recognize the types of protection switching performed by Alcatel-Lucent 1665 DMX
- Describe the features that are available to monitor and maintain Alcatel-Lucent 1665 DMX

Related procedures

For related procedures, refer to Chapter 5, "Trouble-clearing procedures" in this document.

System maintenance using the *WaveStar*® CIT

Overview

The Alcatel-Lucent 1665 DMX shelf is controlled using a PC and a PC-based control program. The two are collectively referred to as the *WaveStar*® Craft Interface Terminal (or *WaveStar*® CIT). Using the *WaveStar*® CIT, maintenance personnel can control and monitor the performance of a Alcatel-Lucent 1665 DMX shelf, either

- locally using a serial line and one of the two RS-232 serial ports on the shelf, or
- remotely using the Alcatel-Lucent 1665 DMX TCP/IP or OSI interface via one of the two LAN ports on the shelf.

WaveStar® CIT introduction

The *WaveStar*® CIT provides three basic methods for controlling the Alcatel-Lucent 1665 DMX shelf using either the

- TL1 command-line interface (cut-through)
- graphical user interface (GUI)

Reference

Refer to Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27) in Chapter 6, "Supporting procedures" for additional information about the *WaveStar*® CIT.

Maintenance philosophy

Overview

Alcatel-Lucent 1665 DMX allows operation and maintenance of network elements in a network from a centralized location. Alcatel-Lucent 1665 DMX continuously monitors the equipment and incoming signals, and reports any current or potential troubles. This enables the user to take the appropriate corrective action.

Types of maintenance

Alcatel-Lucent 1665 DMX supports proactive and reactive maintenance.

Proactive maintenance

Proactive maintenance refers to the process of detecting degrading conditions not severe enough to initiate protection switching or alarming, but indicative of an impending failure.

Proactive maintenance consists of monitoring performance parameters associated with within the network and monitoring. Alcatel-Lucent 1665 DMX also monitors Ethernet parameters such as bytes and frames.

Proactive maintenance consists of monitoring performance parameters associated with the following:

- SONET (for example, OC-N) sections, lines, and paths
- non-SONET (for example, DS1 and DS3) lines and paths
- OTS/OCH/OTU2 lines and ODU2 channels
- Ethernet/Data bytes and frames

Reactive maintenance

Reactive maintenance occurs after a failure. The LEDs on the circuit pack faceplates report internal troubles. Most troubles can be detected and corrected at this level. The optical network (ON) craft interface terminal (CIT) or TL1 interface may be used to TL1 interface may be used to retrieve detailed reports about alarms and conditions. Alcatel-Lucent 1665 DMX can also be configured for TCP/IP interface conforming with standard IEEE 802.3.

Maintenance signals

Overview

Alcatel-Lucent 1665 DMX provides maintenance signaling compliant with the SONET standard (ANSI T1.105) and GR-253-CORE. When Alcatel-Lucent 1665 DMX detects failure conditions on transmission signals, maintenance signals are inserted into the transmission signals in the upstream or downstream direction to notify other network elements.

Alcatel-Lucent 1665 DMX supports the following SONET maintenance signals:

- Alarm indication signals (AIS)
- Remote failure indicator (RFI)
- Path unequipped signals
- Idle signals

Alcatel-Lucent 1665 DMX also supports the following Optical Transport Network (OTN) layer maintenance signals:

- Server Signal Fail (SSF)
- Backward Defect Indicator (BDI)
- Open Connection Indication (OCI)
- Locked (LCK)

Alarm indication signals (AIS)

Alarm indication signals (AIS) notify downstream equipment that a failure has been detected and alarmed by some upstream equipment. Alcatel-Lucent 1665 DMX generates the following alarm indication signals:

- Line AIS (AIS-L): For SONET Lines, loss of signal (LOS) and loss of frame (LOF) are the defects that cause the line terminating equipment (LTE) to send a line alarm indication signal (AIS-L) downstream.
- STS Path AIS (AIS-P): For SONET STS Paths, loss of pointer (LOP-P) and unequipped (UNEQ-P) are the defects that cause the path terminating equipment (PTE) to send an STS Path alarm indication signal (AIS-P) downstream.
- VT Path AIS (AIS-V): For SONET VT Paths, loss of pointer (LOP-V) and unequipped path (UNEQ-V) are the defects that cause the path terminating equipment (PTE) to send an VT Path alarm indication signal (AIS-V) downstream.

Remote failure indicator (RFI)

When downstream terminating equipment detects a defect (see below for explanation of the defects), the terminating equipment sends a remote defect indication (RDI) upstream to the node that originated the signal. After receiving an RDI that persists for two seconds

(± 0.5), the originating node (upstream node), generates a remote failure indicator (RFI) alarm. Alcatel-Lucent 1665 DMX generates the following remote defect indication signals:

- For SONET Lines, loss of signal (LOS), loss of frame (LOF), and alarm indication signal (AIS-L) are the defects that cause the line terminating equipment (LTE) to send an RDI-L back upstream to the originating LTE which then declares an `inc. OCN RFI-L` on the line.
- For SONET STS Paths, loss of pointer (LOP-P), unequipped (UNEQ-P), and alarm indication signal (AIS-P) are the defects that cause the path terminating equipment (PTE) to send an RDI-P back upstream to the originating PTE which then declares an `inc. STSN RFI-P` on the STS path.
- For SONET VT Paths, loss of pointer (LOP-V), unequipped path (UNEQ-V), and alarm indication signal (AIS-V) are the defects that cause the path terminating equipment (PTE) to send an RDI-V back upstream to the originating PTE which then declares an `inc. VT RFI-V` on the VT path.

  Important! RFI-P and RFI-V are not reported at non-path terminating points because they are not actionable and because the impacted service is not terminated at that node.

Path unequipped signals

Alcatel-Lucent 1665 DMX supports STS-N and VT1.5 path unequipped signals. Path unequipped signals are transmitted to notify downstream equipment that the path is incomplete (for example, the absence of a valid cross-connection).

Idle signals

Alcatel-Lucent 1665 DMX supports DS3 (path) idle signals. DS3 idle signals are transmitted to notify downstream equipment that the path is not used or incomplete (for example, the absence of a valid cross-connection).

Server signal failure (SSF) signal

The server signal failure (SSF) signal alerts the downstream client sublayer that a defect or equipment failure has been detected by the upstream server layer. It is sent to the client sublayer and is considered a defect when received.

Backward defect indication (BDI)

The backward defect indication (BDI) signal alerts upstream nodes that a defect or equipment failure has been detected downstream. It is sent within the same layer and is considered a defect when received.

Open connection indication (OCI)

The open connection indication (OCI) signal alerts downstream nodes that an upstream connection is not connected.

Locked (LCK)

The locked (LCK) signal alerts downstream nodes that an upstream connection is administratively locked and no signal is passed through.

Alarm and status conditions reporting

Overview

Alcatel-Lucent 1665 DMX continuously monitors its internal condition and incoming signals according to the state of the tributaries and ports.

Fault detection

If a port or tributary is in the IS (in service) state, Alcatel-Lucent 1665 DMX monitors the port/tributary and activates the appropriate indicators when a failure occurs. Refer to Chapter 2, "Alarm list" for a complete list of alarms and status conditions.

Table 4-1 Monitored and detected incoming signal failure conditions

Incoming Signals	Monitored/Detected Failures
DS1[1]	inc. (from DSX) DS1 AIS inc. (from DSX) DS1 LOF inc. (from DSX) DS1 LOS inc. (from DSX) DS1 RAI inc. (from DSX) DS1 sig. failed (BER) inc. (from fiber) DS1 AIS inc. (from fiber) DS1 LOF inc. (from fiber) DS1 RAI
DS1 sync. ref.	inc. DS1 sync. ref. AIS inc. DS1 sync. ref. BER inc. DS1 sync. ref. EOOF inc. DS1 sync. ref. LOF inc. DS1 sync. ref. LOS inc. DS1 sync. ref. OOL

Table 4-1 Monitored and detected incoming signal failure conditions (continued)

Incoming Signals	Monitored/Detected Failures
DS3[2]	inc. (from DSX) DS3 AIS inc. (from DSX) DS3 IDLE inc. (from DSX) DS3 LOF inc. (from DSX) DS3 LOS inc. (from DSX) DS3 RAI inc. (from DSX) DS3 sig. failed (BER) inc. (from fiber) DS3 AIS inc. (from fiber) DS3 LOF inc. (from fiber) DS3 RAI inc. DS3 CBit Mismatch
E1	inc. (from DSX) E1 AIS inc. (from DSX) E1 LOF inc. (from DSX) E1 LOS inc. (from DSX) E1 sig. failed (BER) incoming CRC-4 MFA mismatch
E1 sync. ref.	inc. E1 sync. ref. AIS inc. E1 sync. ref. BER inc. E1 sync. ref. CRC-4 MFA mismatch inc. E1 sync. ref. LOF inc. E1 sync. ref. LOS inc. E1 sync. ref. OOL
EC-1	inc. EC1 line AIS inc. EC1 LOF inc. EC1 LOS inc. EC1 RFI-L inc. EC1 sig. failed (BER) inc. EC1 sig. degrade (BER) inc. STS LOP

Table 4-1 Monitored and detected incoming signal failure conditions (continued)

Incoming Signals	Monitored/Detected Failures
Fast Ethernet Gigabit Ethernet	inc. FELAN ANM inc. FELAN FEFI inc. FELAN LOS inc. GELAN ANM inc. GELAN LOS
Data	inc. LOS inc. Loss of Synch
OC-3 OC-12 OC-48 OC-192	inc. OCN line AIS inc. OCN LOF inc. OCN LOS inc. OCN RFI-L inc. OCN sig. degrade (BER) inc. OCN sig. failed (BER)
OC-N sync. ref.	inc. line sync. ref. OOL
OCH	inc. MUX OCH LOS-P
ODU2	inc. ODU2 BDI inc. ODU2 DEG inc. ODU2 LCK inc. ODU2 OCI inc. ODU2 SSF
OTS	inc. OTS LOS-P
OTU2	inc. OTU2 BDI inc. OTU2 DEG inc. OTU2 LOF inc. OTU2 LOM inc. OTU2 LOS-P inc. OTU2 SSF

Table 4-1 Monitored and detected incoming signal failure conditions (continued)

Incoming Signals	Monitored/Detected Failures
STS-1 STS-3c STS-12c STS-48c STS-192c	inc. STSN AIS inc. STSN LOP inc. STSN RFI-P inc. STSN sig. degrade (BER) inc. STSN sig. failed (BER) inc. STSN unequipped
VCG	inc. VCG failed inc. VCG LFD inc. VCG LOA
VC-12	inc. VC TU-AIS inc. VC TU-LOP inc. VC LP-RFI inc. VC unequipped
VT1.5	inc. VT AIS inc. VT LOP inc. VT RFI-V inc. VT sig. degrade (BER) inc. VT unequipped

Notes:

1. The BER thresholds for DS1 are based on bipolar 8-zero substitution (B8ZS) or alternate mark inversion (AMI) violations depending on line coding.
2. The BER thresholds for DS3 are based on bipolar 3-zero substitution (B3ZS) coding violations.

Fault isolation

When a failure is detected, Alcatel-Lucent 1665 DMX employs automatic diagnostics to isolate the failed circuit pack or signal. Most failures are isolated to an incoming signal failure (inc. sig. failed) or to a single circuit pack, but some failures may be isolated to more than one circuit pack. Failures are reported to the local technician and operations systems so that repair decisions can be made. If desired, operations system personnel and the local technician can use the *WaveStar*® CIT to gain more detailed information on the trouble condition.

Fault reporting

All failures detected and isolated by Alcatel-Lucent 1665 DMX are stored and made available to be reported, on demand, through the *WaveStar*® CIT. In addition, a history of the past 12000 notifications is maintained and available for on-demand reporting. Each alarm notification is date and time stamped.

If the diagnostic determines that a circuit pack has failed, the red **FAULT** LED on that circuit pack is turned on. If the diagnostic determines that a pluggable transmission module has failed, the port LED associated with the pluggable transmission module is turned on.

If an incoming electrical/optical signal fails, the red **FAULT** LED on the affected circuit pack flashes on and off in one-second intervals. If the circuit pack is equipped with pluggable transmission modules, the port LED associated with the pluggable transmission module flashes on and off in one-second intervals.

Alcatel-Lucent 1665 DMX provides alarm-generate delays and alarm-clear delays. The alarm-generate delay is the time in seconds that the system waits before reporting an incoming signal alarm condition. This prevents transient failures from causing unnecessary maintenance activity. The office alarms are not activated, and the operating systems (OSs) are not notified until a failure lasts at least as long as the alarm-generate delay.

The alarm-clear delay is the time in seconds that the system waits before reporting an equipment alarm condition is cleared. Signal failures have a fixed 10-second delay. Alarm-clear delays prevent premature clearing of alarms. Alarm indications are not cleared until a fault condition has been clear for at least as long as the alarm-clear delay.

Service affecting (SA) vs. non-service affecting (NSA)

Alcatel-Lucent 1665 DMX declares an alarm service affecting (SA) or non-service affecting (NSA) based on protection switch status, cross-connection status, and entity states. A condition is declared NSA (non-service affecting) if the system is successfully providing protection switching in response to the condition, or if the failed entity (circuit pack or signal) is in the standby (not active) state. If protection switching is not successful, or if the entity is unprotected, the condition is declared SA (service affecting).

Alarm masking

Alcatel-Lucent 1665 DMX automatically masks (suppresses the reporting of) secondary or consequential conditions, allowing the operator to quickly identify the root cause of a problem and the services that are affected.

To minimize the number of alarm conditions reported by an NE, related alarms/status conditions are arranged in hierarchical groups. When more than one alarm or status condition in a hierarchical group exists in a single NE, only the top level condition in that hierarchy is reported.

Pre-existing lower-level alarms within a hierarchical group are masked (cleared from the alarm list) when a higher level alarm is detected and reported.

Alarm severity assignment profiles (ASAPs)

Overview

Alarm severity assignment profiles (ASAPs) provide flexibility and control over alarm reporting.

The ASAPs allow users to perform the following:

- create multiple ASAPs for each ASAP type. ASAP types are predefined categories or types of alarms and cannot be changed. Each ASAP type has a DEFAULT ASAP and may have user-created ASAPs. The system supports up to 127 user-created ASAPs (excludes DEFAULT ASAPs).
- provision alarm severity levels for each probable cause within each ASAP.
- assign an ASAP to an entity within the system.

Alarm severity levels

The following alarm severity levels may be assigned to each probable cause within an ASAP.

- Critical (CR)
- Major (MJ)
- Minor (MN)
- Not Alarmed (NA)
- Not Reported (NR).

Not alarmed (NA) and Not reported (NR) severity levels are not supported for non-volatile memory related alarms.

ASAP types and DEFAULT ASAPs

The system provides the following predefined ASAP types with DEFAULT ASAPs.

- "1+1 Bidirectional Protection Group ASAP Type" (p. 4-16)
- "1+1 Optimized Protection Group ASAP Type" (p. 4-16)
- "BLSR Protection Group ASAP Type" (p. 4-17)
- "Data Port ASAP Type" (p. 4-18)
- "DS1 Port ASAP Type" (p. 4-18)
- "DS3 Port ASAP Type" (p. 4-19)
- "E1 Port ASAP Type" (p. 4-19)
- "EC1 Port ASAP Type" (p. 4-20)
- "Circuit Pack ASAP Type" (p. 4-21)
- "Fast Ethernet Port ASAP Type" (p. 4-21)

1+1 Bidirectional Protection Group ASAP Type

Table 4-2 1+1 Bidirectional Protection Group ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level
`Protection switching byte failure`	Major (MJ)
`Protection switching channel match failure`	Major (MJ)
`Automatic protection switch mode mismatch`	Major (MJ)
`Far-end protection line failure`	Major (MJ)

1+1 Optimized Protection Group ASAP Type

Table 4-3 1+1 Optimized Protection Group ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level
`Protection switching byte failure`	Major (MJ)
`Protection switching channel match failure`	Major (MJ)

Table 4-3 1+1 Optimized Protection Group ASAP Type - DEFAULT ASAP (continued)

Probable Cause	Default Alarm Severity Level
Automatic protection switch mode mismatch	Major (MJ)
Automatic protection switch primary section mismatch	Major (MJ)
Automatic protection switch unused codes	Major (MJ)
Automatic protection switch unresolved transient codes	Major (MJ)

BLSR Protection Group ASAP Type

Table 4-4 BLSR Protection Group ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level
Circuit Provisioning Error	Minor (MN)
Default K-bytes	Major (MJ)
Duplicate Ring Node	Major (MJ)
Improper APS Codes	Major (MJ)
Inconsistent APS Codes	Major (MJ)
Inconsistent Ring Prot Mode	Major (MJ)
Node ID Mismatch	Major (MJ)
NUT Inconsistent XC Granularity	Minor (MN)
Path Integrity Failure	Major (MJ)
Ring Ckt Validation Suspended	Minor (MN)
Ring Comm Failure	Minor (MN)
Ring Incomplete	Major (MJ)
Ring Prot Switching Suspended	Major (MJ)
Squelch Data Unavailable	Minor (MN)
Squelch Map Inconsistent	Minor (MN)

Data Port ASAP Type

Table 4-5 Data Port ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
`inc. LOS`	Critical (CR)	Minor (MN)
`inc. Loss of Synch`	Critical (CR)	Minor (MN)
`AUTO link shutdown`	Not Alarmed (NA)	-

DS1 Port ASAP Type

Table 4-6 DS1 Port ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
`inc. (from DSX) DS1 LOS`	Not Alarmed (NA)	Not Alarmed (NA)
`inc. (from DSX) DS1 LOF`	Not Alarmed (NA)	Not Alarmed (NA)
`inc. (from DSX) DS1 AIS`	Not Alarmed (NA)	Not Alarmed (NA)
`inc. (from DSX) DS1 sig. failed`	Not Alarmed (NA)	Not Alarmed (NA)
`inc. (from DSX) DS1 RAI`	-	Not Alarmed (NA)
`inc. (from fiber) DS1 LOF`	-	Not Alarmed (NA)
`inc. (from fiber) DS1 AIS`	-	Not Alarmed (NA)
`inc. (from fiber) DS1 RAI`	-	Not Alarmed (NA)

DS3 Port ASAP Type

Table 4-7 DS3 Port ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
inc. (from DSX) DS3 LOS	Critical (CR)	Critical (CR)
inc. (from DSX) DS3 LOF	Critical (CR)	Critical (CR)
inc. (from DSX) DS3 AIS	Critical (CR)	Critical (CR)
inc. (from DSX) DS3 sig. failed	Critical (CR)	Critical (CR)
inc. (from DSX) DS3 IDLE	Critical (CR)	Critical (CR)
inc. DS3 Cbit Mismatch	Critical (CR)	Critical (CR)
inc. (from DSX) DS3 RAI	-	Not Alarmed (NA)
inc. (from fiber) DS3 LOF	-	Not Alarmed (NA)
inc. (from fiber) DS3 AIS	-	Not Alarmed (NA)
inc. (from fiber) DS3 RAI	-	Not Alarmed (NA)
PROTN DS3 Port Failure	-	Not Alarmed (NA)

E1 Port ASAP Type

Table 4-8 E1 Port ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
inc. (from DSX) E1 LOS	Not Alarmed (NA)	Not Alarmed (NA)
inc. (from DSX) E1 LOF	Not Alarmed (NA)	Not Alarmed (NA)
inc. (from DSX) E1 AIS	Not Alarmed (NA)	Not Alarmed (NA)

Table 4-8 E1 Port ASAP Type - DEFAULT ASAP (continued)

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
inc. (from DSX) E1 sig. failed	Not Alarmed (NA)	Not Alarmed (NA)
incoming CRC-4 MFA mismatch	-	Not Alarmed (NA)

EC1 Port ASAP Type

Table 4-9 EC1 Port ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
inc. EC1 LOS	Critical (CR)	Critical (CR)
inc. EC1 LOF	Critical (CR)	Critical (CR)
inc. EC1 line AIS	Critical (CR)	Critical (CR)
inc. EC1 RFI-L	-	Not Reported (NR)
inc. EC1 sig. degrade (BER)	Critical (CR)	Critical (CR)
inc. EC1 sig. failed (BER)	Critical (CR)	Critical (CR)
inc. EC1 section trace identifier mismatch	Major (MJ)	Minor (MN)
inc. EC1 section trace identifier mismatch, diagnostic	-	Minor (MN)
PROTN EC1 Port Failure	-	Not Alarmed (NA)

Circuit Pack ASAP Type

Table 4-10 Circuit Pack ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
CP contributing to a pack failure	-	Not Alarmed (NA)
CP removed or CP failure	Critical (CR)	Minor (MN)
CP not allowed - eqpt	-	Minor (MN)
CP not allowed - crs	-	Minor (MN)
CP failed	Critical (CR)	Minor (MN)
illegal CP type	-	Minor (MN)
Incompatible CP version	-	Minor (MN)
NP audit failed	Critical (CR)	Minor (MN)
Segment audit failed LAN in	Critical (CR)	-
Segment audit failed LAN out	Minor (MN)	-
unexpected CP type	Critical (CR)	Minor (MN)
version mismatch	-	Minor (MN)
Protection CP Input fault	-	Minor (MN)

Fast Ethernet Port ASAP Type

Table 4-11 Fast Ethernet Port ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
AUTO link shutdown	Not Alarmed (NA)	-
Exceeded MTU size drop	-	Minor (MN)
ERP - Multiple RPL Owners	Major (MJ)	-

Table 4-11 Fast Ethernet Port ASAP Type - DEFAULT ASAP (continued)

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
ERP - PDU WatchDog Timeout	Major (MJ)	-
inc. FE-LAN ANM	Critical (CR)	-
inc. FE-LAN FEFI	Not Reported (NR)	-
inc. FE-LAN LOS	Critical (CR)	-
Member Not Collecting/ Distributing	Not Alarmed (NA)	-
Segment audit failed LAN in	Critical (CR)	-
Segment audit failed LAN out	Critical (CR)	-
STP autolock port disable	Major (MJ)	-

Gigabit Ethernet Port ASAP Type

Table 4-12 Gigabit Ethernet Port ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
AUTO link shutdown	Not Alarmed (NA)	-
Exceeded MTU size drop	-	Minor (MN)
ERP - Multiple RPL Owners	Major (MJ)	-
ERP - PDU WatchDog Timeout	Major (MJ)	-
inc. GE-LAN LOS	Critical (CR)	Minor (MN)
ECV - excessive code violation	Minor (MN)	-
inc. GE-LAN ANM	Critical (CR)	Minor (MN)
Member Not Collecting/ Distributing	Not Alarmed (NA)	-

Table 4-12 Gigabit Ethernet Port ASAP Type - DEFAULT ASAP (continued)

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
`inc. Loss of Synch`	Critical (CR)	Minor (MN)
`Segment audit failed LAN in`	Critical (CR)	-
`Segment audit failed LAN out`	Critical (CR)	-
`STP autolock port disable`	Major (MJ)	-

Link Aggregation Group ASAP Type

Table 4-13 Link Aggregation Group ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level
`inc. LAG Partial Link Loss`	Minor (MN)
`inc. LAG Total Link Loss`	Critical (CR)
`inc. LAG PLCF`	Not Reported (NR)
`STP autolock port disable`	Major (MJ)

Non-Volatile Memory Module ASAP Type

Table 4-14 Non-Volatile Memory Module ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level
`NVM failed`	Critical (CR)
`NVM removed or NVM failed`	Critical (CR)

OCH Port ASAP Type

Table 4-15 OCH Port ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
`inc. MUX OCH LOS-P`	Critical (CR)	-

OCn Port ASAP Type

Table 4-16 OCn Port ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
inc. OCN LOS	Critical (CR)	Minor (MN)
inc. OCN LOF	Critical (CR)	Minor (MN)
inc. OCN line AIS	Critical (CR)	Not Alarmed (NA)
inc. OCN RFI-L	-	Not Reported (NR)
inc. OCN sig. degrade (BER)	Critical (CR)	Minor (MN)
inc. OCN sig. failed (BER)	Critical (CR)	Minor (MN)
inc. line sync. ref. OOL	Minor (MN) (active)	Minor (MN) (standby)
inconsistent DCC values	-	Major (MJ)
neighbor SYSCTL CP unavailable	-	Major (MJ)
section DCC channel failed	-	Minor (MN)
inc. OCN section trace identifier mismatch	Major (MJ)	Minor (MN)
inc. OCN section trace identifier mismatch, diagnostic	-	Minor (MN)
line DCC channel failed	-	Minor (MN)
ENNI signaling communications failure with peer	-	Minor (MN)

ODU2 Tributary ASAP Type

Table 4-17 ODU2 Tributary ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
`inc. ODU2 BDI`	-	Not Alarmed (NA)
`inc. ODU2 DEG`	Critical (CR)	Minor (MN)
`inc. ODU2 LCK`	Critical (CR)	Minor (MN)
`inc. ODU2 OCI`	Critical (CR)	Minor (MN)
`inc. ODU2 SSF`	Critical (CR)	Minor (MN)

OTS Port ASAP Type

Table 4-18 OTS Port ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
`inc. OTS LOS-P`	Critical (CR)	Minor (MN)

OTU2 Port ASAP Type

Table 4-19 OTU2 Port ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
`inc. OTU2 BDI`	-	Not Alarmed (NA)
`inc. OTU2 DEG`	Critical (CR)	Minor (MN)
`inc. OTU2 LOF`	Critical (CR)	Minor (MN)
`inc. OTU2 LOM`	Critical (CR)	Minor (MN)
`inc. OTU2 LOS-P`	Critical (CR)	Minor (MN)
`inc. OTU2 SSF`	Critical (CR)	Minor (MN)

Pluggable Transmission Module ASAP Type

Table 4-20 Pluggable Transmission Module ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
unexpected or failed Pluggable Transmission Module	Critical (CR)	Minor (MN)
Pluggable Transmission Module removed	Critical (CR)	Minor (MN)
Pluggable Transmission Module insufficient maximum rate	Critical (CR)	Minor (MN)

STS Ring Channel ASAP Type

Table 4-21 STS Ring Channel ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
inc. STSN LOP	Critical (CR)	Minor (MN)
inc. STSN AIS	Critical (CR)	Minor (MN)
inc. STSN unequipped	Critical (CR)	Minor (MN)
inc. STSN sig. degrade (BER)	Critical (CR)	Minor (MN)
inc. STSN sig. failed (BER)	Critical (CR)	Minor (MN)
inc. STSN RFI-P	-	Not Reported (NR)

Subshelf ASAP Type

Table 4-22 Subshelf ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level
Subshelf Communication Failed	Major (MJ)
Subshelf initialziation IP	Not Alarmed (NA)

System ASAP Type

Table 4-23 System ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level
`AGNE communication failure`	Major (MJ)
`NSAP count in L1 overflowed`	Major (MJ)
`NSAP count in L1 threshold crossed`	Minor (MN)
`Power/Fuse Failure`	Minor (MN)
`excessive holdover`	Minor (MN)

System Timing ASAP Type

Table 4-24 System Timing ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Unprotected	Protected
`inc. SRC`[1] `sync. ref. LOS`	Major (MJ)	Minor (MN)
`inc. SRC`[1] `sync. ref. LOF`	Major (MJ)	Minor (MN)
`inc. SRC`[1] `sync. ref. OOL`	Major (MJ)	Minor (MN)
`inc. SRC`[1] `sync. ref. AIS`	Major (MJ)	Minor (MN)
`inc. SRC`[1] `sync. ref. BER`	Major (MJ)	Minor (MN)
`inc. SRC`[1] `sync. ref. EOOF`	Major (MJ)	Minor (MN)
`inhibit switch`	-	Minor (MN)
`inc. SRC`[1] `sync. ref. CRC-4 MFA mismatch`	Major (MJ)	Minor (MN)

Notes:

1. DS1 or E1 depending on the external reference signal.

VC12 Ring Channel ASAP Type

Table 4-25 VC12 Ring Channel ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
`inc. VC TU-LOP`	Major (MJ)	-
`inc. VC TU-AIS`	Major (MJ)	-
`inc. VC LP-RFI`	-	Not Reported (NR)
`inc. VC unequipped`	Major (MJ)	-

VCG Port ASAP Type

Table 4-26 VCG Port ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
`Exceeded MTU size drop`	-	Minor (MN)
`ERP - Multiple RPL Owners`	Major (MJ)	-
`ERP - PDU WatchDog Timeout`	Major (MJ)	-
`inc. VCG failed`	Critical (CR)	Minor (MN)
`VCG Loss of Partial Capacity`	Minor (MN)	Minor (MN)
`VCG Failure of LCAS Protocol (Sink)`	Minor (MN)	Minor (MN)
`VCG Failure of LCAS Protocol (Source)`	Minor (MN)	Minor (MN)
`Remote client signal failed`	Not Alarmed (NA)	-
`Segment audit failed VCG in`	Critical (CR)	Minor (MN)
`Segment audit failed VCG out`	Critical (CR)	Minor (MN)
`STP autolock port disable`	Major (MJ)	Minor (MN)

VCG STS Tributary ASAP Type

Table 4-27 VCG STS Tributary ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
`Member Signal Unacceptable – LCAS`	Minor (MN)	Minor (MN)

VCG VT1.5 Tributary ASAP Type

Table 4-28 VCG VT1.5 Tributary ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level
`Member Signal Unacceptable – LCAS`	Minor (MN)

VT1.5 Ring Channel ASAP Type

Table 4-29 VT1.5 Ring Channel ASAP Type - DEFAULT ASAP

Probable Cause	Default Alarm Severity Level	
	Service Affecting (SA)	Non-Service Affecting (NSA)
`inc. VT LOP`	Major (MJ)	Minor (MN)
`inc. VT AIS`	Major (MJ)	Minor (MN)
`inc. VT unequipped`	Major (MJ)	Minor (MN)
`inc. VT sig. degrade (BER)`	Major (MJ)	Minor (MN)
`inc. VT RFI-V`	-	Not Reported (NR)

Provisioning ASAPs

The system supports the following ASAP provisioning functions:

- **Creating ASAPs**: New ASAPs may be created for each ASAP type. The system supports up to 127 user-created ASAPs (does not include the DEFAULT ASAPs). Once 127 user-created ASAPs are created, an existing ASAP must be deleted before a new ASAP can be created.
- **Changing ASAPs**: The system supports changing user-created ASAP names (cannot change DEFAULT ASAP names) and the alarm severity levels within each user-created and DEFAULT ASAP. The system also supports restoring the default alarm severity levels within an ASAP.
- **Deleting ASAPs**: The system supports deleting a user-created ASAP that is not currently active. DEFAULT ASAPs cannot be deleted.

For more information about provisioning ASAPs, refer to *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.

Assigning ASAPs

The associated DEFAULT ASAP is assigned to an entity when the entity is created (for example, when a slot is equipped). Users cannot pre-assign an ASAP to an entity before the entity is created.

After an ASAP is created, it can be assigned to a specific entity within the shelf. Different ASAPs within an ASAP type may be assigned to different entities within the shelf; however, only one ASAP may be assigned to an entity at a time. Assigning a different ASAP to an entity overrides the previous assignment.

For more information about assigning ASAPs, refer to *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.

Protection switching

Overview

Alcatel-Lucent 1665 DMX provides different types of protection switching, described in the subsequent sections of this chapter:

- "2-Fiber bidirectional line-switched ring (BLSR) switching" (p. 4-34)
- "Unidirectional path-switched ring switching" (p. 4-40)
- "1+1 line protection switching" (p. 4-43)
- "1+1 optimized line protection switching" (p. 4-47)
- "1+1 bidirectional line protection switching" (p. 4-49)
- "1+1 equipment protection switching" (p. 4-51)
- "Spanning tree" (p. 4-53)
- "Resilient Packet Ring (RPR) switching" (p. 4-54)
- "Ethernet ring protection" (p. 4-56)
- "Synchronization reference protection switching" (p. 4-58)

Application modes

The following provisionable application modes are available for optical ports:

- BLSR: The BLSR application mode provides revertive, bidirectional ring line protection switching on low-speed OC-48 interfaces and high-speed OC-48 and OC-192 interfaces (main OC-48 and OC-192 OLIUs).
- UPSR: The UPSR application mode provides unidirectional STS-N/VT1.5 ring path protection switching on low-speed OC-3, OC-12, and OC-48 interfaces and high-speed OC-12, OC-48, and OC-192 interfaces. This option supports single- and dual-homed ring-on-ring topologies.
- 1+1: The 1+1 application mode provides revertive/nonrevertive SONET 1+1 protection for OC-3, OC-12, OC-48, and OC-192 interfaces.
- 1+1 optimized: The 1+1_OPTM application mode provides bidirectional 1+1 protection for OC-3, OC-12, OC-48, and OC-192 interfaces.
- 1+1 bidirectional: The 1+1_BIDIR application mode, provides revertive/nonrevertive bidirectional 1+1 protection for OC-3, OC-12, OC-48, and OC-192 interfaces.

- 0x1S1 (non-VLF mains): The 0x1 Side 1 application mode is an unprotected mode used on low-speed OC-N interfaces when protection is not desired. All traffic is transmitted and received on the line in slot 1 of the function unit group. Side 2 is not monitored, and is not necessarily equipped. For example, socket 3 of an LNW49 in Slot 2 does not need to be equipped with a pluggable transmission module if the port pair 3 is provisioned as 0x1S1. However, if the socket 3 is equipped on Side 2, a system idle signal (STS UNEQ-P or AIS-P) is transmitted to the far-end. This option is user-provisionable on a per-port basis and supports dual-homed ring-on-ring topologies.
- 0x1S2 (non-VLF mains): The 0x1 Side 2 application mode is an unprotected mode used on low-speed OC-N interfaces when protection is not desired. All traffic is transmitted and received on the line in slot 2 of the function unit group. Side 1is not monitored, and is not necessarily equipped. For example, socket 4 of an LNW49 in Slot 1 does not need to be equipped with a pluggable transmission module if the port pair 4 is provisioned as 0x1S2. However, if the socket 4 is equipped on Side 1, a system idle signal (STS UNEQ-P or AIS-P) is transmitted to the far-end. This option is user-provisionable on a per-port basis and supports dual-homed ring-on-ring topologies.
- 0x1 (VLF mains): The 0x1 application mode is an unprotected mode used on high-speed and low-speed OC-N interfaces when protection is not desired.

From the *WaveStar®* CIT System View menu, select **Configuration** → **Equipment** to set the protection modes.

Mixed protection modes

Alcatel-Lucent 1665 DMX supports mixed protection modes (for example, UPSR, 1+1, or 1+1_BIDIR) on different ports of the same OLIU. For example, the quad OC-3 interface could have two ports provisioned for 1+1 mode and one for UPSR mode. Protection modes cannot be mixed on the same OLIU port.

Ethernet interface protection

On the WAN (SONET) side of the network, Alcatel-Lucent 1665 DMX provides protection via an STS-n/VT1.5 UPSR configuration (for point-to-point applications) or an IEEE 802.1W rapid spanning tree protocol.

Provisioning protection switching

From the *WaveStar®* CIT System View menu, select **Fault** → **Protection Switch** to provision protection switching.

A popup window then appears offering a choice of the switch protected devices on the shelf. The type of protection switching provisioned for each device is shown next to the device location.

Double clicking on one of the protection groups calls up the elements of the group or a second popup display offering a choice of user-defined protection switch modes.

The choices are as follows:

- 1+1 Equipment Protection (Circuit Pack): Inhibit, Forced, Manual (Normal), or Reset.
- 1+1 Line Protection (Port): Lockout, Forced to Working, Forced to Protection, Manual to Working, Manual to Protection, or Reset.
- 1+1 Optimized Line Protection (Port): Lockout, Forced, or Reset.
- 1+1 Bidirectional Line Protection (Port): Lockout, Forced, Manual, or Reset.
- 2F BLSR: Clear; Lockout of Protection, Span; Force to Protection, Ring; Manual to Protection, Ring.
- Path Protection: Lockout, Manual, Forced, or Clear

Selecting a switching mode and clicking the Apply button at the bottom of the screen enables the switching mode in the selected device.

2-Fiber bidirectional line-switched ring (BLSR) switching

Introduction

The Alcatel-Lucent 1665 Data Multiplexer system performs 2-fiber bidirectional line-switched ring (BLSR) protection switching in response to automatically detected faults in OC-48 or OC-192 lines and external commands from the *WaveStar*® CIT or operations system (OS). For more information about **Fault** → **Protection Switch**, refer to the on-line help available from the *WaveStar*® CIT.

Ring definition

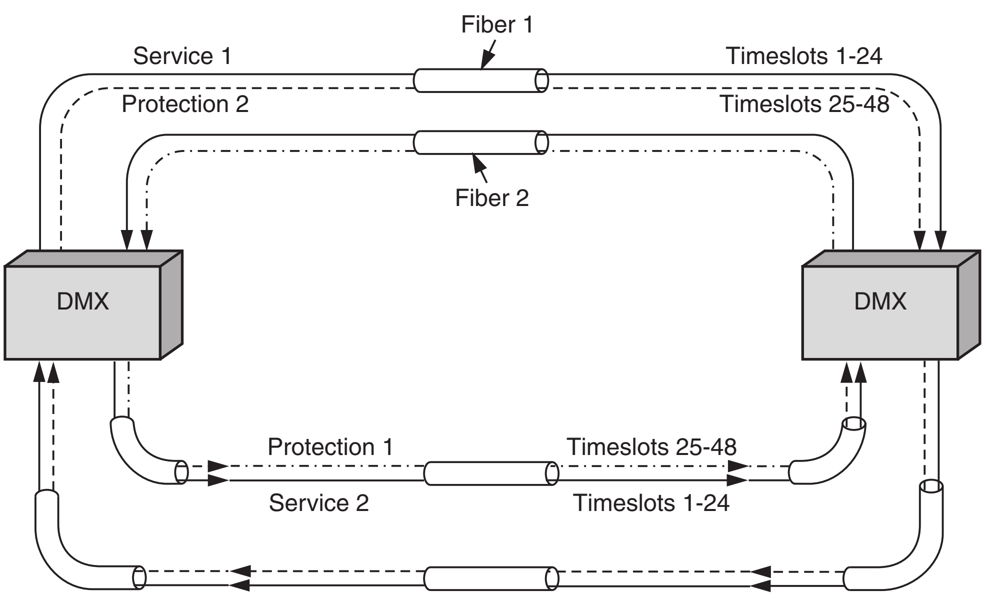
A ring is a collection of nodes that form a closed loop, where each node is connected to the adjacent nodes. BLSRs provide redundant bandwidth and/or equipment to ensure system integrity in the event of any transmission failure, including a fiber cut or node failure.

2-fiber OC-48 BLSR traffic capacity

In a 2-fiber OC-48 BLSR, each bidirectional OC-48 line carries 24 STS-1 equivalent timeslots of service capacity (1–24) and 24 STS-1 equivalent timeslots of protection capacity (25–48).

Figure 4-1, "Traffic capacity in an 2-fiber OC-48 BLSR" (p. 4-34) illustrates the service and protection traffic capacities in a 2-fiber OC-48 BLSR.

Figure 4-1 Traffic capacity in an 2-fiber OC-48 BLSR

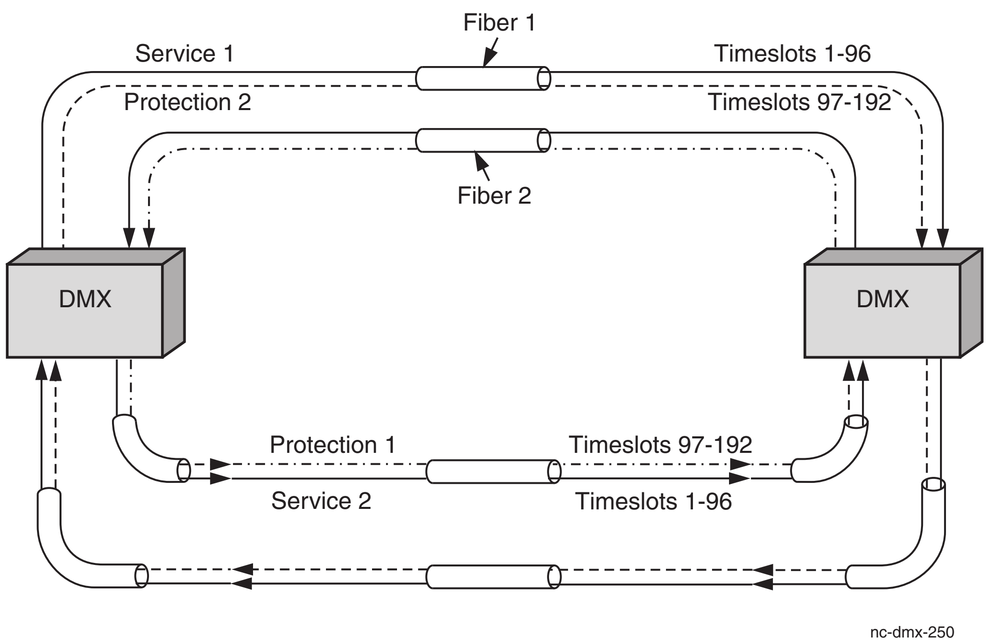


2-fiber OC-192 BLSR traffic capacity

In a 2-fiber OC-192 BLSR, each bidirectional OC-192 line carries 96 STS-1 equivalent timeslots of service capacity (1–96) and 96 STS-1 equivalent timeslots of protection capacity (97–192).

Figure 4-2, "Traffic capacity in an 2-fiber OC-192 BLSR" (p. 4-35) illustrates the service and protection traffic capacities in a 2-fiber OC-192 BLSR.

Figure 4-2 Traffic capacity in an 2-fiber OC-192 BLSR



Switch request priorities

Important! If a higher or equal priority switch request exists, a new switch request is denied.

The following table shows the 2-fiber BLSR protection switch priorities (in descending order of priority).

Table 4-30 Protection switching priorities (BLSR)

Switch Priorities (Descending Order)	Source of Request
Clear[1]	*WaveStar*® CIT or OS
Lockout of Protection - Span	*WaveStar*® CIT or OS
Forced of Service to Protection, Ring	*WaveStar*® CIT or OS
Signal Fail - Ring	Automatic
Signal Degrade - Ring	Automatic

Table 4-30 Protection switching priorities (BLSR) (continued)

Switch Priorities (Descending Order)	Source of Request
Manual Switch to Protection - Ring	*WaveStar*® CIT or OS
Wait to Restore	Automatic
Reverse Request - Ring	Automatic
No Request	Automatic

Notes:

1. The Clear request does not affect Signal Fail, Signal Degrade, Reverse Request, or No Request.

Bidirectional revertive protection switching

The optical line uses bidirectional revertive 2-fiber ring protection switching. Bidirectional refers to protection switching that is performed in the transmit and receive directions simultaneously. The traffic switches from the working tributaries of one line to the protection tributaries of the line in the opposite direction when a fault is detected. In revertive switching when the fault and wait-to-restore interval clear, the traffic switches back (reverts) to the working tributaries.

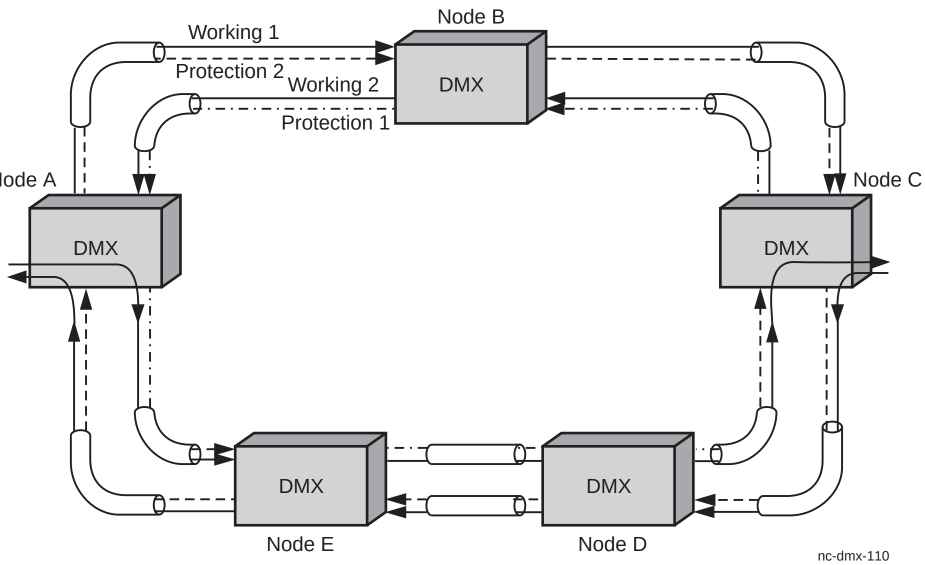
Self-healing rings

A 2-fiber BLSR is a self-healing (transport is automatically restored after node or fiber failures) ring configuration in which traffic is bidirectional between each pair of adjacent nodes and is protected by redundant bandwidth on the bidirectional lines that interconnect the nodes in the ring. Because traffic flow is bidirectional between the nodes, traffic can be added at one node and dropped at the next without traveling around the entire ring. This capability leaves the spans between other nodes available for additional traffic. Therefore, with distributed traffic patterns, a bidirectional line-switched ring can carry more traffic than the same facilities could carry if configured for a unidirectional path-switched ring. Additionally, you can use the protection capacity to provide unprotected transport for extra traffic when no failures are present. Up to 16 nodes are supported on a ring. Each OC-48 line carries 24 STS-1 equivalent timeslots of working capacity plus 24 STS-1 equivalent timeslots of protection capacity. Each OC-192 line carries 96 STS-1 equivalent timeslots of working capacity plus 96 STS-1 equivalent timeslots of protection capacity. In the event of a fiber or node failure, service is restored by switching traffic from the working capacity of the failed line to the protection capacity in the opposite direction around the ring. (See Figure 4-3, “ Normal traffic flow in a 2-fiber BLSR” (p. 4-37) and Figure 4-4, “Loopback protection switch in a 2-fiber BLSR” (p. 4-38).)

2-fiber BLSR traffic flow

The figure below shows normal (non-protection-switched) traffic flow on a 2-fiber BLSR.

Figure 4-3 Normal traffic flow in a 2-fiber BLSR



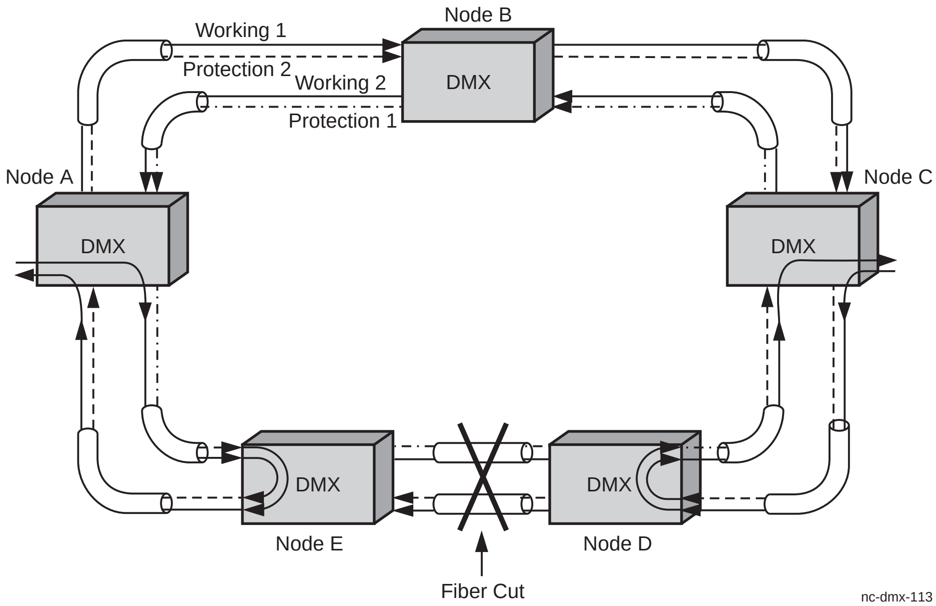
Protection switching

When a line failure triggers a protection switch, the nodes adjacent to the failure switch traffic on to protection capacity. Traffic heading toward the failure is looped back on to the protection capacity traveling away from the failure to reach its destination by traveling the opposite way around the ring (see the figure below). Service is reestablished on the protection capacity in less than 50 milliseconds after detection of the failure (for catastrophic failures in rings without existing protection switches or extra traffic).

Fiber cut example

Figure 4-4, "Loopback protection switch in a 2-fiber BLSR" (p. 4-38) illustrates a 2-fiber BLSR protection switch that results from a fiber cut.

Figure 4-4 Loopback protection switch in a 2-fiber BLSR



Protection traffic flow

For 2-fiber ring protection switching, the nodes adjacent to the failure make connections to bridge the add and through traffic to the protection tributaries of the line in the other direction. All drop and through traffic is selected from the protection tributaries of the line in the other direction.

In the figure above, traffic going from Node A to Node C that normally passes through Node E and Node D on "working 2" capacity is switched at Node E on to the "protection 2" capacity of the line leaving Node E in the direction of Node A. The traffic loops back through Nodes A, B, and C to Node D where it is looped back to Node C. Similarly, traffic going from Node C to Node A that normally passes through Node D and Node E on "working 1" capacity is switched at Node D on to the "protection 1" capacity of the line leaving Node D in the direction of Node C. The traffic loops back through Nodes C, B, and A to Node E where it is looped back to Node A. Note that only the nodes adjacent to the failure perform loopback protection switches. The same approach is used for a node failure. For example, if Node D fails, Nodes C and E perform loopback protection switches to provide an alternate route for ring traffic.

Extra traffic

Alcatel-Lucent 1665 DMX supports extra traffic on high-speed (main) 2-fiber OC-48 and in systems with OC-192 VLF mains, extra traffic is supported on OC-192 BLSRs in the mains and FNs. The extra traffic capability allows the protection channels to carry additional low-priority traffic during fault-free conditions.

The extra traffic is established by provisioning cross-connections to the high-speed (main) BLSR protection channels. Provisioning cross-connections on the protection channels is only supported on high-speed BLSRs. Pass through cross-connections are provisioned on the protection channels at intermediate nodes. (Protection channels that are not carrying Extra Traffic are terminated at the intermediate nodes.)

If a BLSR protection switch occurs, traffic is switched from the working channels to the protection channels and extra traffic is preempted.

If extra traffic circuits are preempted, AIS-P is used to squelch the circuits. When the BLSR protection switch clears, the extra traffic is restored.

NUT

Non-preemptible unprotected traffic is traffic carried on (working and/or protection) BLSR channels for which protection switching has been provisioned as disabled. As the name implies, NUT is unprotected and not preempted in the event of a protection switch.

BLSR protocols allow the available bandwidth of a BLSR to be partitioned into three types of channels:

- working channel to carry working traffic.
- protection channel which may be used to carry extra traffic.
- NUT channel to carry non-preemptible unprotected traffic.

Working traffic is protected against failure events via the BLSR APS protocol, while extra traffic is unprotected traffic carried on the protection channels. Any failure event that may require the protection channels for protection purposes shall preempt the extra traffic. NUT carried on non-preemptible unprotected channels affords a higher level of survivability as compared to extra traffic, which is preempted during a protection switch, but a lower level of survivability as compared to working traffic, which is carried on its corresponding protection channel during a protection switch. Note that non-preemptible unprotected traffic is not considered extra traffic.

Important! Alcatel-Lucent 1665 DMX supports NUT on 2-fiber OC-48 and OC-192 BLSRs.

Unidirectional path-switched ring switching

Introduction

Alcatel-Lucent 1665 DMX supports path switched ring applications in accordance with the path protection switching schemes described in Telcordia Technologies GR-1400.

UPSR is the Alcatel-Lucent 1665 DMX default mode. Alcatel-Lucent 1665 DMX performs UPSR switching in response to automatically detected faults in paths and external commands from a *WaveStar*® CIT or operations system (OS). Alcatel-Lucent 1665 DMX supports UPSR switching for VT1.5 and STS-N signals on OC-N interfaces (OC-3/OC-12/OC-48/OC-192 OLIUs).

Path protection switching functions are available from the *WaveStar*® CIT System View menu when you select **Fault** → **Protection Switch**.

Protection switching priorities

The following table shows the UPSR protection switch priorities (in descending order of priority).

Table 4-31 Protection switch priorities (UPSR)

Switch Priorities (Descending Order)	Source of Request
Clear	*WaveStar*® CIT or OS
Lockout	*WaveStar*® CIT or OS
Forced	*WaveStar*® CIT or OS
Automatic Switch: Signal Failed	Automatic
Automatic Switch: Signal Degrade	Automatic
Manual	*WaveStar*® CIT or OS

Automatic path selector criteria

Alcatel-Lucent 1665 DMX performs automatic UPSR switching based on the automatic path selector criteria. The automatic path selector criteria uses the following hierarchy of signal impairments (ordered from top to bottom in increasing signal quality):

- line LOS, LOF, AIS, STS and VT path AIS, LOP, and UNEQ (most impaired - worst signal quality)
- STS-N Path BER exceeding a signal fail threshold
- STS-N and VT Path BER exceeding a signal degrade threshold
- Path-level signal with no impairments.

Important! Alcatel-Lucent 1665 DMX selects the path-level signal with the best quality.

Unidirectional switching

Unidirectional switching refers to protection switching that is performed in the receive direction only. The transmitting terminal transmits the same path-level signal on two paths. The receiving terminal monitors the two path-level signals independently and chooses one path-level signal as the active path and the other path-level signal as the standby path. Alcatel-Lucent 1665 DMX selects the incoming path-level signal with the best quality (based on the automatic path selector criteria).

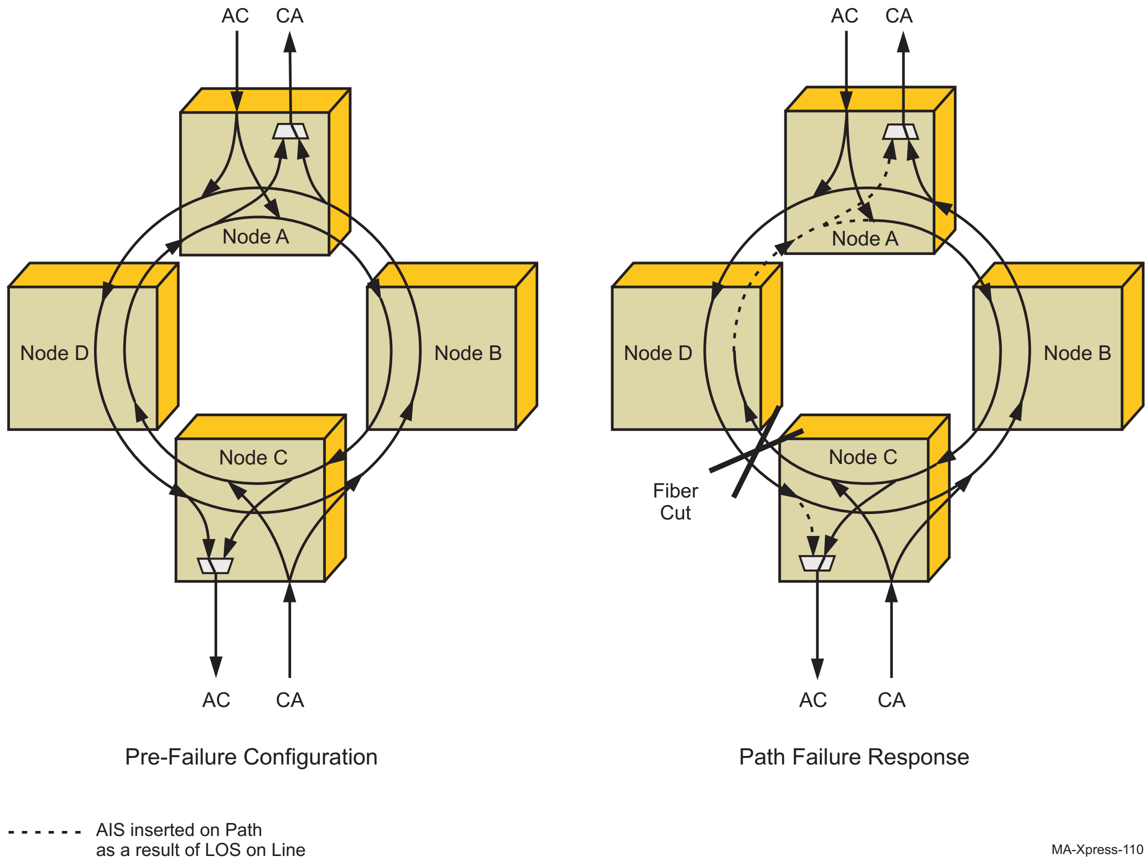
Nonrevertive switching

UPSR switching is nonrevertive. When a protection switch occurs, the receiving terminal selects the signal from the standby path. In nonrevertive switching, when the fault clears the receiving terminal does *not* switch back to the original path.

UPSR architecture

Figure 4-5, “UPSR switching example” (p. 4-42) illustrates an example of UPSR protection switching. The UPSR switching is performed in the receive direction. If the active incoming path-level signal fails, the circuit pack chooses the standby path-level signal. In the transmit direction, the circuit pack bridges the same path-level signal to the working and protection paths.

Figure 4-5 UPSR switching example



Path protection rings feed a SONET payload (STS-N or VT) from the ring entry point, simultaneously in both rotations of the ring, to the signal's ring drop or exit point as shown by traffic AC and CA. This duplication of the signal that enters the ring is called a "head-end bridge." The node that drops the signal from the ring monitors both ring rotations and is responsible for selecting the signal that has the highest quality based on LOS, LOF, path AIS, LOP, STS-N/VT unequipped, and STS-N/VT path BER performance. This function at the ring exit point is called a "tail-end switch."

1+1 line protection switching

Introduction

Alcatel-Lucent 1665 DMX supports SONET standard 1+1, unidirectional, revertive/nonrevertive line protection switching on OC-3, OC-12, OC-48, and OC-192 optical interfaces. Protection switches are initiated by automatically detected faults in the circuit packs/optical lines and/or by external commands from the *WaveStar®* CIT or OS interface.

1+1 protection switching is provisioned using the *WaveStar®* CIT System View **Configuration** → **Equipment** menu and the supporting displays.

Automatic line protection

In multispan applications each OC-N span switches independently. For example, in hubbing applications, a switch on the central office-to-hub span does not cause switches on any of the hub-to-remote spans. Similarly, a line switch on a hub-to-remote span will not propagate to other hub-to-remote or central office-to-hub spans.

1+1 application mode

To support a 1+1 protection compatibility, the OC-N interface must be provisioned to the 1+1 mode by selecting **Configuration** → **Equipment**.

Line protection switching can also be controlled by selecting**Fault** → **Protection Switch**.

For more information on setting up protection switching, refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.

Revertive/nonrevertive operation

The Alcatel-Lucent 1665 DMX supports user-provisioned revertive/nonrevertive operation. In revertive operation, the system reverts back to the original active line when the fault condition or switch request clears. In nonrevertive operation, the system does not revert back to the original active line when the fault condition or switch request clears. The original active line becomes the standby line and the original standby line becomes the active line.

For more information about provisioning revertive/nonrevertive operation refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.

Protection switching priorities

Alcatel-Lucent 1665 DMX supports a system-wide 1+1 protection switch priority for optical interfaces. The priority parameter (UNIPROTPRIO) is provisioned by selecting **Configuration** → **Equipment**, then highlighting DMX, clicking Select, and provisioning 1+1 Protection Priority to be Forced or Signal Failure.

Nonrevertive 1+1 Switch Priority = Forced

The following table lists the nonrevertive 1+1 line protection switch priorities (in descending order of priority) when the switch priority is provisioned as Forced. When Forced (default) is selected, a forced switch is not preempted by a failure of the protection line in 1+1 applications.

Table 4-32 Protection switching priorities (nonrevertive 1+1 switch priority = forced)

Switch Priorities (Descending Order)	Source of Request
Reset	*WaveStar*® CIT or OS (clears any user-initiated switch request)
Lockout of Protection	*WaveStar*® CIT or OS prevents any switch request (automatic or user-initiated)
Forced Switch	*WaveStar*® CIT or OS
Signal Failure	Automatic
Signal Degrade	Automatic
Manual Switch	*WaveStar*® CIT or OS

Revertive 1+1 Switch Priority = Forced

The following table lists the revertive 1+1 line protection switch priorities (in descending order of priority) when the switch priority is provisioned as Forced. When Forced (default) is selected, a forced switch is not preempted by a failure of the protection line in 1+1 applications (Revertive Mode = Enabled).

Table 4-33 Protection switching priorities (revertive 1+1 switch priority = forced)

Switch Priorities (Descending Order)	Source of Request
Reset	*WaveStar*® CIT or OS (clears any user-initiated switch request)
Lockout of Protection	*WaveStar*® CIT or OS prevents any switch request (automatic or user-initiated)
Forced Switch	*WaveStar*® CIT or OS
Signal Failure	Automatic
Signal Degrade	Automatic
Manual Switch	*WaveStar*® CIT or OS

Table 4-33 Protection switching priorities (revertive 1+1 switch priority = forced) (continued)

Switch Priorities (Descending Order)	Source of Request
Wait to Restore	Automatic
Reverse Request	Automatic
No Request	Automatic

Nonrevertive 1+1 Switch Priority = Signal Failure

The following table lists the nonrevertive 1+1 line protection switch priorities (in descending order of priority) when the switch priority is provisioned as Signal Failure. When Signal Failure is selected, a signal failure on the protection side preempts a forced switch in 1+1 applications

Table 4-34 Protection switching priorities (nonrevertive 1+1 switch priority = signal failure)

Switch Priorities (Descending Order)	Source of Request
Reset	*WaveStar*® CIT or OS (clears any user-initiated switch request)
Lockout of Protection	*WaveStar*® CIT or OS prevents any switch request (automatic or user-initiated)
Signal Failure (Protection)	Automatic
Forced Switch	*WaveStar*® CIT or OS
Signal Failure (Working)	Automatic
Signal Degrade	Automatic
Manual Switch	*WaveStar*® CIT or OS

Revertive 1+1 Switch Priority = Signal Failure

The following table lists the revertive 1+1 line protection switch priorities (in descending order of priority) when the switch priority is provisioned as Signal Failure. When Signal Failure is selected, a signal failure on the protection side preempts a forced switch in 1+1 applications (Revertive Mode = Enabled).

Table 4-35 Protection switching priorities (revertive 1+1 switch priority = signal failure)

Switch Priorities (Descending Order)	Source of Request
Reset	*WaveStar*® CIT or OS (clears any user-initiated switch request)
Lockout of Protection	*WaveStar*® CIT or OS prevents any switch request (automatic or user-initiated)
Signal Failure (Protection)	Automatic
Forced Switch	*WaveStar*® CIT or OS
Signal Failure (Working)	Automatic
Signal Degrade	Automatic
Manual Switch	*WaveStar*® CIT or OS
Wait to Restore	Automatic
Reverse Request	Automatic
No Request	Automatic

1+1 optimized line protection switching

Introduction

Alcatel-Lucent 1665 DMX supports 1+1 optimized, bidirectional, nonrevertive line protection switching on OC-3, OC-12, OC-48, and OC-192 optical interfaces. Protection switches are initiated by automatically detected faults in the circuit packs/optical lines and/or by external commands from the *WaveStar®* CIT or OS interface.

1+1 optimized protection switching is provisioned using the *WaveStar®* CIT System View **Configuration** → **Equipment** menu and the supporting displays.

1+1_OPTM application mode

To support a 1+1 optimized protection compatibility, the OC-3, OC-12, OC-48, OC-192 interface must be provisioned to the 1+1 optimized mode for 1+1 applications by selecting **Configuration** → **Equipment**.

Line protection switching can also be controlled by selecting **Fault** → **Protection Switch**.

For more information on setting up protection switching, refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.

Wait to rename

Alcatel-Lucent 1665 DMX supports a system-wide 1+1_OPTM Wait to Rename parameter. The parameter is provisioned by selecting the **Configuration** → **Equipment**, then highlighting DMX, clicking Select, and provisioning an interval of 0 to 60 minutes (5 minutes is the default).

The Wait to Rename parameter is equivalent to the wait-to-rename timer in revertive protection switching. When the event that caused the protection switch is cleared, and after a subsequent delayed interval (the wait-to-restore interval) the line carrying service is switched back to its pre-protection switch configuration. The non-revertive operation of 1+1 optimized protection is achieved by interchanging the "Primary" and "Secondary" role designations of the lines after the switch event has cleared and after wait-to-rename interval expires.

Protection switching priorities

The following table lists the 1+1 optimized line protection switch priorities (in descending order of priority).

Table 4-36 Protection switching priorities (1+1 optimized)

Switch Priorities (Descending Order)	Source of Request
Clear	*WaveStar*® CIT or OS (clears any user-initiated switch request)
Lockout	*WaveStar*® CIT or OS
Local Signal Failure or Signal Degrade on the secondary section	Automatic
Forced Switch to the secondary section	*WaveStar*® CIT or OS
Signal Failure on the primary section	Automatic
Signal Degrade on the primary section	Automatic
Wait to Rename	Automatic

1+1 bidirectional line protection switching

Introduction

Alcatel-Lucent 1665 DMX supports 1+1 bidirectional, revertive/nonrevertive line protection switching on OC-3, OC-12, OC-48, and OC-192 optical interfaces. Protection switches are initiated by automatically detected faults in the circuit packs/optical lines and/or by external commands from the *WaveStar*® CIT or OS interface.

1+1 bidirectional protection switching is provisioned using the *WaveStar*® CIT System View **Configuration** → **Equipment** menu and the supporting displays.

1+1_BIDIR application mode

To support a 1+1 bidirectional protection compatibility, the OC-3, OC-12, OC-48, and OC-192 interface must be provisioned to the *1+1 bidirectional* mode by selecting **Configuration** → **Equipment**.

Line protection switching can also be controlled by selecting **Fault** → **Protection Switch**.

For more information on setting up protection switching, refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.

Revertive/nonrevertive operation

The Alcatel-Lucent 1665 DMX supports user-provisioned revertive/nonrevertive operation. In revertive operation, the system reverts back to the original active line when the fault condition or switch request clears. In nonrevertive operation, the system does not revert back to the original active line when the fault condition or switch request clears. The original active line becomes the standby line and the original standby line becomes the active line.

For more information about provisioning revertive/nonrevertive operation refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.

Protection switching priorities

The following table shows the nonrevertive 1+1 bidirectional line protection switch priorities (in descending order of priority).

Table 4-37 Protection switching priorities (nonrevertive 1+1 bidirectional)

Switch Priorities (Descending Order)	Source of Request
Reset	*WaveStar*® CIT or OS (clears any user-initiated switch request)

Table 4-37 Protection switching priorities (nonrevertive 1+1 bidirectional) (continued)

Switch Priorities (Descending Order)	Source of Request
Lockout of Protection	*WaveStar*® CIT or OS prevents any switch request (automatic or user-initiated)
Signal Failure (Protection)	Automatic
Forced Switch	*WaveStar*® CIT or OS
Signal Failure (Working)	Automatic
Signal Degrade	Automatic
Manual Switch	*WaveStar*® CIT or OS

The following table shows the revertive 1+1 bidirectional line protection switch priorities (in descending order of priority).

Table 4-38 Protection switching priorities (revertive 1+1 bidirectional)

Switch Priorities (Descending Order)	Source of Request
Reset	*WaveStar*® CIT or OS (clears any user-initiated switch request)
Lockout	*WaveStar*® CIT or OS prevents any switch request (automatic or user-initiated)
Signal Failure (Protection)	Automatic
Forced Switch	*WaveStar*® CIT or OS
Signal Failure (Working)	Automatic
Signal Degrade	Automatic
Manual Switch	*WaveStar*® CIT or OS
Wait to Restore	Automatic
Reverse Request	Automatic
No Request	Automatic

1+1 equipment protection switching

Introduction

Alcatel-Lucent 1665 DMX provides optional, nonrevertive, 1+1 equipment protection on all non-Ethernet electrical interface circuit packs. The 1+1 equipment protection switching takes place in response to automatically detected faults and external commands from the *WaveStar*® CIT or operations system (OS). Protection switching is provisioned using the *WaveStar*® CIT System View **Configuration** → **Equipment** menu and the supporting displays.

Protection switching priorities

The following table lists the 1+1 equipment protection switch priorities (in descending order of priority).

Table 4-39 Protection switching priorities (1+1 equipment protection)

Switch Priorities (Descending Order)	Source of Request
Reset	*WaveStar*® CIT or OS clears any user-initiated switch request
Inhibit Switch	*WaveStar*® CIT or OS prevents any switch request (automatic or user-initiated)
Forced Switch	*WaveStar*® CIT or OS switch to standby
Automatic Switch	Automatic
Manual (Normal) Switch	*WaveStar*® CIT or OS switch to standby

1+1 nonrevertive protection switching

In 1+1 nonrevertive protection switching, the Main OLIUs (M1 and M2) receive signals from the same "active" function unit circuit pack (either in slot 1 or slot 2). One side is active and the other side is in standby. Green ACTIVE LEDs on the faceplates of these circuit packs indicate which packs are active. When a protection switch occurs, the standby side now becomes the active side. The original active side becomes the standby side. The status remains the same (nonrevertive) after the fault clears.

Unprotected equipment

If protection is not desired, SONET interfaces can be provisioned for no protection by equipping only slot 1 of a Function Unit group with a particular circuit pack. For example, if slot 1 of a Function Unit is equipped with a 12DS3/EC1 circuit pack, then slot 2 must be equipped with the appropriate apparatus blank.

Autolock

Alcatel-Lucent 1665 DMX supports a system-wide autolock for 1+1 protected equipment switching (Mains and electrical low-speed interfaces). The feature is provisioned by selecting **Configuration** → **Equipment**, then highlighting DMX, clicking Select, and provisioning the count to anything but 0, and the switch and release intervals.

Count

Specifies the maximum number of consecutive non-pack-removal equipment switches allowed in the provisioned switch interval before the group is put into the autolock state.

Values are from 0 to 20. The default is 0 which disables the function.

The autolock count clears when the autolock release timer expires, when an INHIBIT, FRCD or NORM **`sw-toprotn`** switch command or a **`sw-towkg`** switch command is issued, or when a pack is removed from the group, whichever occurs first.

When the autolock count or switch interval is re-provisioned, any autolock counts that have not yet effected an autolock will be cleared and restarted.

Switch interval

Specifies the time interval (1 to 1440 minutes) for the maximum number of non-pack-removal equipment switches (provisioned under Count) to occur before the protection group is put into the autolock state. The default is 25 minutes.

The autolock switch interval begins when the first switch occurs. When the oldest counted switch is earlier than the provisioned interval, it is no longer counted, and the interval then begins with the next oldest switch.

Release interval

Specifies the maximum time interval (1 to 1440 minutes) the group is in the autolock state. The default is 1440 minutes (24 hours).

The autolock state clears when this autolock release timer expires, when an INHIBIT or FRCD SW-TOPROTN switch command or a SW-TOWKG RESET switch command is issued, or when a pack is removed from the group, whichever occurs first.

Reprovisioning of the autolock release interval has no effect on existing autolock release timers.

Spanning tree

Overview

The spanning tree algorithm and protocol simplifies the configuration and connection of an active network topology from the arbitrarily connected components of a bridged LAN. Frames are forwarded through some of the bridge ports in the bridged LAN and not through others held in a blocking state. At any time, the bridges created effectively connect the LANs to which ports in a forwarding state are attached. Frames are forwarded both directions through bridge ports that are in the forwarding state. The ports in a blocking state do not forward frames in either direction but may be but may included in the active topology.

Algorithm

The spanning tree algorithm and its associated bridge protocol operate to support and maintain the quality of MAC service. In order to perform this function, the algorithm:

- Configures the active topology of the bridged LAN into a single spanning tree, so that there is at most one data route between any two end stations. This eliminates data loops.
- Provides for fault tolerance by the automatic reconfiguration of the spanning tree to cope with a bridge failure or a breakdown in a data path within the confines of the bridged LAN components.
- Accommodates the addition of a bridge or bridged port to the LAN components without the formation of any transient data loops.

Reference

For more information on setting up a spanning tree, refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.

Resilient Packet Ring (RPR) switching

Introduction

Alcatel-Lucent 1665 DMX provides revertive RPR protection for Ethernet traffic on the LNW78 100/1G FSR Gigabit Ethernet circuit packs. The RPR protection switching takes place in response to automatically detected faults and external commands from the *WaveStar*® CIT or operations system (OS). Protection switching is provisioned using the *WaveStar*® CIT System View **Configuration** → **Equipment** menu and the supporting displays.

Protection switching priorities

The following table lists the RPR protection switch priorities (in descending order of priority).

Table 4-40 Protection switching priorities (RPR protection)

Switch Priorities (Descending Order)	Source of Request
Reset	*WaveStar*® CIT or OS
Signal Failure	Automatic
Signal Degrade	Automatic
Manual Switch	*WaveStar*® CIT or OS
Wait to Restore	Automatic

Operation

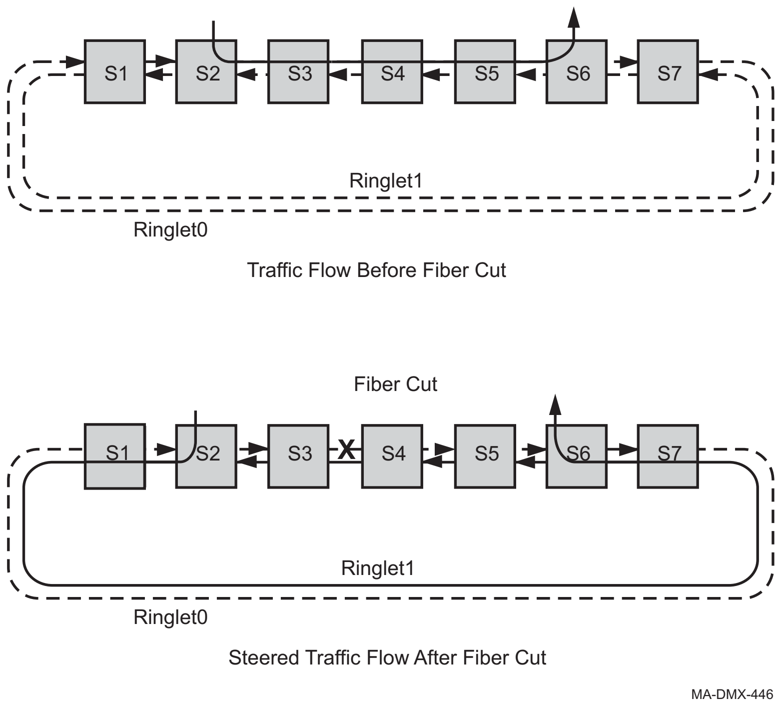
Alcatel-Lucent 1665 DMX supports the steering mechanism for RPR protection switching as defined in the IEEE 802.17 standard. When RPR topology discovery detects a fault in the ring, the topology change is communicated to each node in the ring.

Each node that originates traffic performs a head-end switch that steers traffic onto ringlet 0 or ringlet 1, on a destination node basis, to avoid the failed span. Each node uses its topology image to choose a ringlet. Traffic is reestablished in less than 50 milliseconds after the failure is detected.

The 50-millisecond protection time includes a ring with up to 255 nodes and up to 2000 kilometers in circumference. Protection switching is complete when all the nodes in the ring have been notified of changes in the protection state and start to re-steer traffic away from the fault. Refer to Figure 4-6, "RPR protection switching example" (p. 4-55).

When RPR topology discovery detects the fault has cleared, the topology change is communicated to each node in the ring. When the fault and provisionable wait-to-restore interval clear, the traffic switches back (reverts) to the original ringlet. The RPR protection wait-to-restore timer is provisionable on an RPR span basis using **Configuration** → **Equipment**. For detailed information about provisioning RPR, refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.

Figure 4-6 RPR protection switching example



Ethernet ring protection

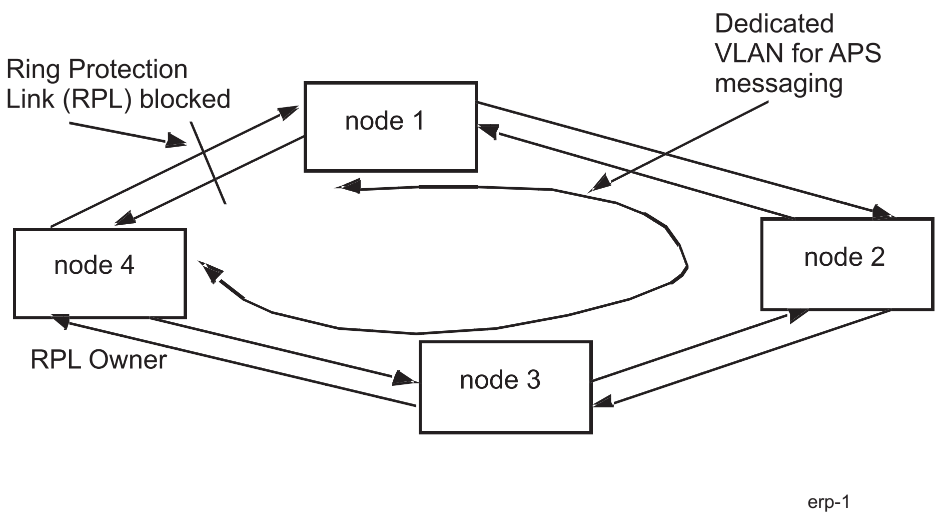
Overview

The LNW70/170 circuit pack supports rapid (50ms) Ethernet ring protection switching for Ethernet links connected in a ring configuration. Ethernet ring protection is provisionable on Fast Ethernet LAN ports, Gigabit Ethernet LAN ports, and VCGs.

Architecture

Figure 4-7, "Ethernet ring protection (normal state)" (p. 4-56) shows a four-node ring. One of the links on node 4 has been provisioned to be the Ring Protection Link (RPL). The provisioned RPL is blocked by default for normal traffic. Node 4 is the RPL Owner, and blocks traffic bidirectionally. Switching is revertive; that is, when a failure clears in the ring, the RPL is blocked (after a wait-to-restore delay).

Figure 4-7 Ethernet ring protection (normal state)

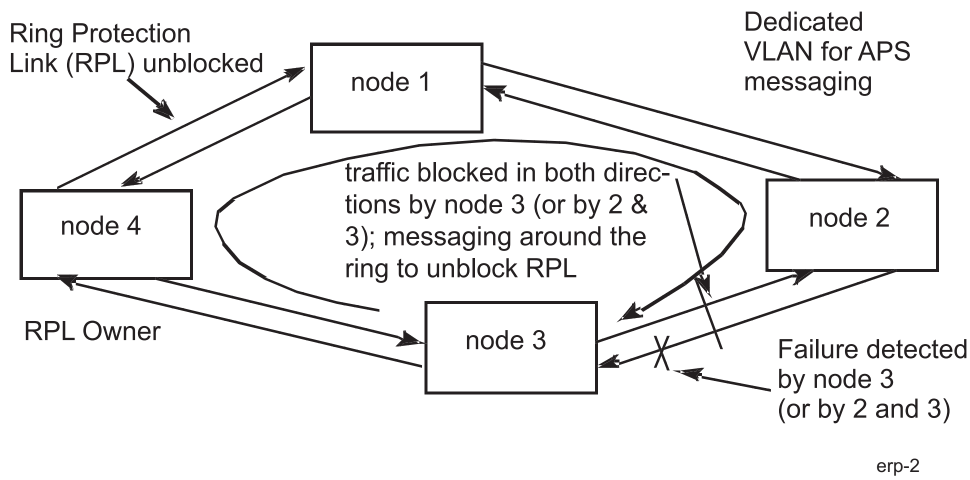


The ring has a VLAN dedicated to APS signaling, called the R-APS channel. Messages are R-APS PDUs. When a change occurs in the ring, 3 R-APS PDUs are sent quickly; otherwise, R-APS PDUs are sent every 5 seconds. Under most conditions, only a single node in the ring is sending R-APS messages.

The link that is blocked in the ring is blocked bidirectionally by the RPL Owner, or by the nodes detecting a failure. The R-APS channel within a blocked link is also partially blocked. It does not forward any messages it receives, but the node can initiate or receive messages.

Figure 4-8, "Ethernet ring protection (failure state)" (p. 4-57) shows the same four-node ring after a failure. The failure may be detected by a single node, or by both nodes connected to the link. The nodes detecting the failure block the failed link bidirectionally, and send signal failure (SF) R-APS messages around the ring. Each node receiving the message flushes its filtering database (unless the R-APS message indicates otherwise). The node that was blocking a link unblocks it.

Figure 4-8 Ethernet ring protection (failure state)



Reference

For more information about provisioning Ethernet ring protection, refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.

Synchronization reference protection switching

Overview

Alcatel-Lucent 1665 DMX provides protection for all system synchronization references. Synchronization reference protection switching occurs in response to automatically detected faults and external commands from an *WaveStar*® CIT or operations system (OS).

Protection switching priorities

The following table shows the synchronization reference protection switch priorities (in descending order of priority).

Table 4-41 Synchronization reference protection switch priorities

Switch Types	Source of Request
Clear Reference Switch (Reset)	*WaveStar*® CIT or OS
Lockout (See Note 1)	*WaveStar*® CIT or OS
Forced Switch (See Note 1)	*WaveStar*® CIT or OS
Reference Failure	Automatic
Manual Switch	*WaveStar*® CIT or OS

Notes:

1. Applicable to DS1/E1 external timing references only.

Operation

In the system Line and External timing modes, synchronization reference protection switching may be provisioned for the following:

- Revertive-1: When provisioned Revertive-1, main-1-1 (Line timing mode) or REF-1 (External timing mode) is designated the primary reference.
- Revertive-2: When provisioned Revertive-2, main-2-1 (Line timing mode) or REF-2 (External timing mode) is designated the primary reference.
- Nonrevertive (default): When a reference is selected, it will remain active even after the other reference recovers from the degradation that caused the protection switch, unless line timing and Sync Autoreconfiguration (auto) is enabled and the other reference has changed to a higher quality.

If neither reference is available, the system automatically switches to the *holdover* timing mode.

When Alcatel-Lucent 1665 DMX is provisioned for synchronization messaging, the system can determine the quality of the line timing references by reading the synchronization messages in the OC-N transport overhead bytes.

If automatic synchronization reconfiguration is enabled, Alcatel-Lucent 1665 DMX automatically selects the highest quality reference. Sync messaging and automatic synchronization reconfiguration can be provisioned using the *WaveStar®* CIT **Configuration** → **Timing/Sync**.

When a manual revertive reference switch is performed, the system reports a standing condition indicating a revertive reference switch is active. A Reset is required to switch back to the designated primary reference and clear the standing condition. When a manual nonrevertive reference switch is performed, the system does not report any standing conditions or alarms since both references are designated for service.

Synchronization mode protection switching

The system can be provisioned to revertive or nonrevertive timing mode switching. If provisioned for revertive mode switching (default), the system automatically switches from holdover mode to the provisioned timing mode (external timing or line timing) when a timing reference failure clears. If provisioned for nonrevertive mode switching, the system must be manually switched from holdover mode to the provisioned timing mode (external timing or line timing) when a timing reference failure clears.

The sources used to supply line timing (any OC-N line, but not on WDM packs) can be manually selected in the Line timing mode.

Timing modes may be provisioned by selecting *WaveStar®* CIT **Configuration** → **Timing/Sync**.

Loopbacks

Introduction

Alcatel-Lucent 1665 DMX provides the following types of loopbacks:

- Low-speed OC-N (OC-3, OC-12, OC-48), DS1, E1, DS3, EC-1 Facility and Terminal loopbacks
- Ethernet Facility and Terminal loopbacks
- Data Terminal loopbacks
- High-speed OC-3, OC-12, OC-48, and OC-192 Facility loopbacks

Loopbacks

Loopbacks can be provisioned using the *WaveStar®* CIT graphical display.

From the *WaveStar®* CIT System View, select **Fault** → **Analysis** → **Loopback** and then select the circuit pack and the desired port. Choose either Facility or Terminal for Loopback Type and click on **Operate** or **Release**. A Command Mode of NORM (Normal) or FRCD (Forced) must also be specified for OC-N loopbacks.

Active port loopbacks are indicated by a continuously lighted **ABN** LED on the SYSCTL circuit pack. Clicking on the **Alarm List** button from the *WaveStar®* CIT System View returns a report that indicates that loopbacks are present.

Facility loopbacks

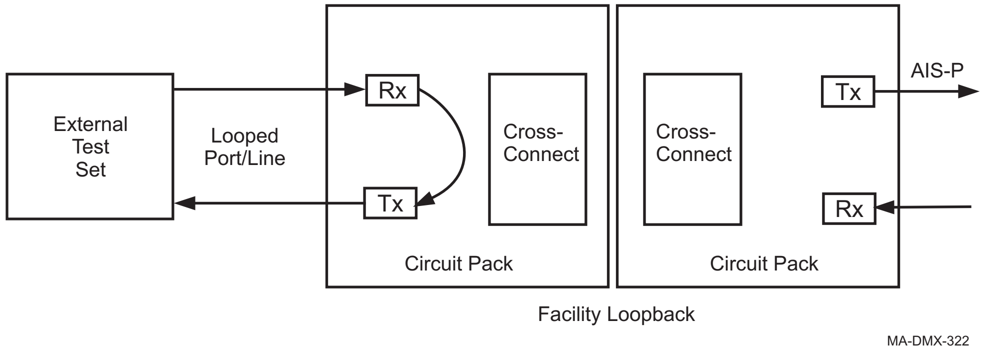
A *Facility* loopback connects the incoming received signal to the transmitter in the return direction. Electrical signals are looped back intact, including BPVs. Optical signals are looped back after the optical to electrical conversion.

Facility loopbacks are supported on the

- low-speed DS1, E1, DS3, and EC-1 electrical ports
- low-speed OC-3, OC-12, and OC-48 optical ports
- high-speed OC-3, OC-12, OC-48, and OC-192 optical ports (M1, M2)
- Ethernet LAN ports
- OC-3, OC-12, and OC-48 client ports on LNW705 XM10G/8 circuit packs

The following figure shows a facility loopback used in a test arrangement with an external test set.

Figure 4-9 Facility loopback example



Reference the following for additional information on facility loopbacks:

- Establishing an OC-N facility loopback may cause switching in UPSR or 1+1 applications. Anything not force switched to the looped-back side will switch, unless the other side is failed.
- In BLSR applications, establishing a facility loopback generates a switch request to switch away from the looped-back side.
- A loopback request to a port is denied if that port/line or a tributary within that line is part of a test access session.
- Optical facility loopbacks operate on an OC-N line AID.
- For OC-N loopbacks, two Command Mode parameters (**NORM** [normal] or **FRCD** [forced]) are available by selecting **Fault** → **Analysis** → **Loopback** → **Facility**. If the Command Mode is NORM, the loopback is denied unless the OC-N line is NMON. If the Command Mode is FRCD, the loopback is accepted (as long as the other parameters are valid).
- For OC-N loopbacks, if the Command Mode is **NORM** and the line is *not* in the NMON state, the command is denied.

Terminal loopbacks

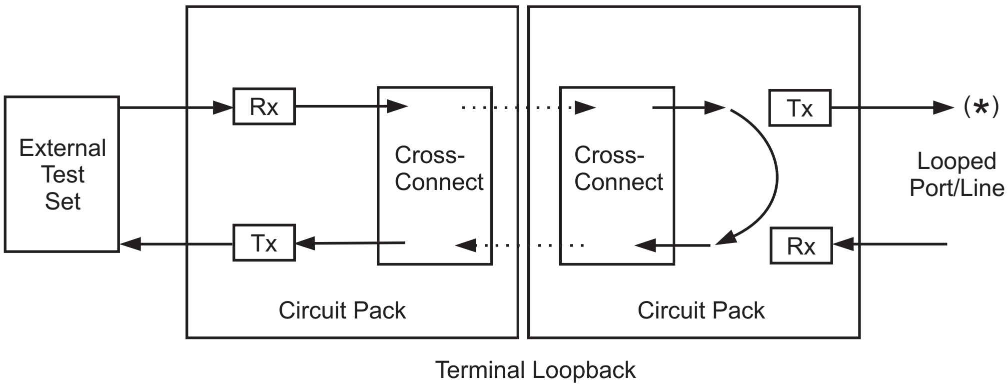
A *Terminal* loopback connects the entire signal that is about to be transmitted back into the associated incoming receiver.

Terminal loopbacks are supported on the

- low-speed DS1, E1, DS3, and EC-1 electrical ports
- low-speed OC-3, OC-12, and OC-48 optical ports
- Data ports
- Ethernet LAN ports and Link Aggregation Groups (LAGs)
- OC-3, OC-12, OC-48, and Ethernet/Data client ports on LNW705 XM10G/8 circuit packs

The following figure shows a terminal loopback used in a test arrangement with an external test set.

Figure 4-10 Terminal loopback example



(*) = See table below for signal transmitted.

If interface type is...	Then signal transmitted is...
DS1	AIS
DS3 (LNW19B and LNW20)	AIS
DS3 (LNW16)	Bridged
SONET	Bridged
Ethernet	Open
Data	Open

MA-DMX-323

Reference the following for additional information on terminal loopbacks:

- In BLSR applications, it is recommended (but not required) that the user lockout protection before establishing the terminal loopback. If not, service may be affected throughout the ring.
- Establishing an OC-N terminal loopback may cause switching in UPSR or 1+1 applications. If all traffic is switched away from the side to be looped back, establishing the loopback is not initially service-affecting.
- A line or path must be switched to the side with the OC-N loopback in order to see the effect of the loopback. In UPSR applications, it is possible to isolate individual paths for testing by switching all traffic away from the looped-back line, then switching the path to be tested to the looped-back line.
- Optical terminal loopbacks operate on an OC-N line AID.
- The only valid value for the Command Mode is **FRCD** for OC-N Terminal loopbacks.
- A loopback request to a port is denied if that port/line or a tributary within that line is part of a test access session.
- On a single Ethernet circuit pack, an ENET loopback is allowed on only one LAN port at a time. Loopbacks are not allowed on VCGs (WAN ports).

- When a loopback is in place, alarms on that port are suppressed (not generated and cleared if present) and PM counting is halted. When the loopback is released, the PM counters are cleared and alarms and PM counting may resume. If the port monitoring mode is provisioned as AUTO, the port is not allowed to transition to in-service (IS) while the loopback is active.
- Changes made to the provisioned values during the loopback using **`ed-eport`** are accepted but do not take effect until the loopback is released.
- The operational parameters of an Ethernet port are forced to the following values while the loopback is active:
  – Duplex Mode = FULL
  – Flow Control Mode = DISABLE
  – Line Rate = 100 M (Fast Ethernet ports only)

Tests

Overview

Alcatel-Lucent 1665 DMX provides the following self tests:

- an LED test
- an IAO LAN test
- a system controller test
- a transmission test.

LED test

The LED test verifies that the SYSCTL and circuit pack faceplate LEDs are operating properly in a shelf. The test consists of one or more test iterations (cycles) repeated as many times as specified. The LED test does not affect the LEDs on the fan unit.

In each test iteration the circuit pack faceplate LEDs (including SYSCTL) are lighted for 10 seconds and turned off for 10 seconds. This repeats for each test iteration specified. The PWR ON LED is always on if the shelf is powered and cannot be tested.

The LEDs revert to normal operation after the LED test is completed.

A LED test can be performed by selecting **Fault** → **Test** → **LED** to test all LEDs on the shelf or the LEDs on an individual circuit pack.

The **ACO TEST** push-button on the SYSCTL circuit pack may also be used to test the LEDs on the shelf.

IAO LAN test

The IntraOffice LAN (IAO LAN) test sets up an internal loopback that is used to verify that the Alcatel-Lucent 1665 DMX shelf's IAO LAN is capable of interfacing with an IAO LAN hub. From the *WaveStar®* CIT System View menu, select **Fault** → **Test** → **IAO LAN**.

System Controller test

The system controller test performs a basic sanity check of the system controller on the SYSCTL circuit pack. The test results in a pass/fail indication of the processor's health.

Select **Fault** → **Test** → **System Controller** from the *WaveStar®* CIT System View menu to test the system controller.

Transmission test

Alcatel-Lucent 1665 DMX provides internal testing capabilities for installation and manual troubleshooting. DS1, DS3, and E1 test signal generators and detectors are integrated in the system, eliminating the need for external test equipment to do DS1/DS3/E1 transmission testing.

Specific signals and system components may be tested. For example, technicians can manually enable the integrated test signal generators and detectors for a DS1, DS3, or E1 low-speed interface.

Select **Fault** → **Test** → **Transmission** from the *WaveStar*® CIT System View menu to test transmission.

Additional popup screens are used to facilitate the specific transmission tests.

Reports

Introduction

Reports provide parameters and status information for a range of equipment. For example, a report may show the parameters for all the transmission ports on a shelf.

Equipment Lists

From the *WaveStar*® CIT System View menu, select **Reports** → **Equipment Lists** → to view reports for

- **Pack** (view details of circuit packs)
- **Pluggable Transmission Module** (view details of the selected pluggable transmission module)
- **Port** (view ports of the selected circuit pack)
- **VCG** (view VCG groups being supported by the selected shelf)
- **Trib** (view tributaries supported by the selected shelf [or device])
- **Misc. Discretes** (view all miscellaneous discretes)

Status Lists

From the *WaveStar*® CIT System View menu, select **Reports** → **Status Lists** → to view detailed status information for

- **Pack** (display circuit pack status and alarm information)
- **Pluggable Transmission Module** (display pluggable transmission module status and alarm information)
- **Port** (display port status, alarm, and fault information)
- **VCG** (display VCG status, alarm, and fault information)
- **Trib** (display tributary status, alarm, and fault information)

Path Protection List

The Path Protection List shows specific information about the UPSRs (for example, current role [active or standby] for the specific AIDs on the ring[s]).

The Path Protection List can be obtained by selecting **Reports** → **Path Protection List**.

BLSR Protection Switch List

The BLSR Protection Switch List shows the protection switch status of the BLSRs on the shelf.

The BLSR Protection Switch List can be obtained by selecting **Reports** → **BLSR Protection Switch List**.

NE Alarm List

The NE Alarm List shows all active alarms on the local network element. The Alarm List can be obtained by clicking the **Alarm List** button in the upper right-hand corner of the System View window.

The identity of the condition (for example, OLIU CP failed, or inc. DS3 sig. failed) is included in the report along with a time stamp indicating when the condition was detected.

This summary contains time and date stamps indicating when each condition was detected and when it cleared. *WaveStar®* CIT events contain a time stamp indicating when the command was entered. Alarm and status entries in the retrieve-history report are not subject to holdoff and clear delay.

Alarm filtering

By selecting **Reports** → **NE Alarm List** or **Fault** → **NE Alarm List**, users can select different categories from the Alarm Selection Panel that filter the alarm list accordingly. For example, only the service affecting alarms can be viewed.

The following table lists the different sorting options available from the Alarm Selection Panel.

Table 4-42 Alarm filtering options

Field	Options
Alarm Category	All
	Facility
	Equipment
	Environment
	Common Equipment

Table 4-42 Alarm filtering options (continued)

Field	Options
Alarm Entity Type	DS1
	E1
	DS3
	EC1
	OC3
	OC12
	OC48
	OC192
	STS1
	STS3C
	STS12C
	STS48C
	STS192C
	VT1.5
	VC12
	Ethernet
	FE
	1GE
	VCG
	Data
Alarm Severity Level	All
	Critical
	Major
	Minor
	Not Alarmed
Effect On Service	All
	Service Affecting
	Non-Service affecting

Remote NE Alarm List

The Remote NE Alarm List shows alarms on remote NEs in the same alarm group. The list includes the TID of the remote NE, the date of the alarm, the AID, the alarm severity level, and a description of the event/alarm.

The Remote NE Alarm List can be retrieved by selecting **Reports** → **Remote NE Alarms List**.

Alarm Severity Assignment Profile User List

The Alarm Severity Assignment Profile User List shows entities that a specified ASAP has been assigned to.

The ASAP User List can be retrieved by selecting **Reports** → **Alarm Severity Assignment Profile User List**.

VT XC Fabric Utilization

The VT XC Fabric Utilization report shows the VT cross-connect fabric utilization for the main and function packs on the shelf.

This report can be retrieved by selecting **Reports** → **XC Fabric Utilization**.

Backplane Bandwidth Utilization

The shows the backplane utilization and VT backplane utilization for any function packs on the shelf.

This report can be retrieved by selecting **Reports** → **Backplane Bandwidth Utilization**.

NE History Log

The NE History Log shows the start and end of alarm and status conditions and all CIT/OS activities that affect the state of the network element. This includes autonomous events such as alarms, protection switching, maintenance conditions, and network element status changes. Select **Reports** → **NE History Log** to obtain an NE History Log.

The network element stores up to 12000 of the most recent events. All entries or only entries for a specified time interval may be retrieved.

NE Security Log

The NE Security Log shows all TL1 provisioning commands and security-related events. For example, user authentication attempts, attempts to access resources, user security changes, network element security changes, and system resets are shown. Select **Reports** → **NE Security Log** to obtain an NE Security Log.

The network element stores up to 10000 of the most recent events. All entries or only entries for a specified time interval may be retrieved.

MAC Address List

The MAC address list shows a current list of MAC addresses, VLAN IDs, and Address Types for a slot AID or for a port AID.

The MAC Address List may be filtered by VLAN ID, MAC Address, and Address Type.

This report can be retrieved by selecting **Reports** → **MAC Address List**.

GbE Line Utilization

The GbE line utilization report shows how much data bandwidth has been used per Ethernet and VCG port. The information generated for the report is based on performance monitoring data. Select **Reports** → **GbE Line Utilization** to obtain a GbE Line Utilization report.

5 Trouble-clearing procedures

Overview

Purpose

This chapter contains the trouble-clearing procedures for the Alcatel-Lucent 1665 Data Multiplexer.

Safety precautions

Many trouble-clearing procedures require actions that are service affecting. These actions are indicated by a caution message indicating the extent of the service disruption. For example:

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Contents

Before you begin

Before you begin

Prior to performing *most* procedures in this chapter,

1. If not previously completed, install generic and *WaveStar*® CIT software on the PC. Refer to Procedure 6-1: "Install software on the PC" (p. 6-4).
2. Connect PC and establish a *WaveStar*® CIT session. Refer to Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27).

Required equipment

Most procedures in this chapter require the following equipment:

- Personal Computer (PC) with *WaveStar*® CIT software installed
- Wrist Strap

  Important! Also refer to the procedure to be performed for other equipment requirements. If other equipment is required to perform a specific procedure, that equipment is listed in the procedure.

Procedure 5-1: Address communication failure with network element

Overview

Use this procedure to address a communications failure with a network element. It is assumed that any alarm-monitoring centers and remote network elements have lost communication with the network element.

Important! This procedure must be performed locally at the network element.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to address a communication failure with a network element.

1 Observe the green power LEDs on the network element. Is at least one green power LED lighted?

If...	Then...
Yes,	Continue with the next step.
No,	Go to Procedure 5-2: " Clear "−48V power/fuse FA or FB failed" alarm" (p. 5-13)

2 Observe the LEDs on the SYSCTL circuit pack faceplate. Are the LEDs constantly cycling?

If...	Then...
Yes,	Go to Step 6.
No,	Continue with the next step.

3 Observe the **IND** display on the SYSCTL circuit pack faceplate. Does the **IND** display show *MPx.x* where *x.x* is the generic number?

If...	Then...
Yes,	The network element can not find a valid generic and/or database and is in the Maintenance Mode state. Perform Procedure 5-44: "Clear "Generic/Database/Equipment Configuration" alarms/conditions" (p. 5-104) to clear the Maintenance Mode condition. STOP! End of Procedure.
No,	Continue with the next step.

4 Press and hold the **ACO TEST** push-button on the SYSCTL circuit pack faceplate. Did all the LEDs on all the circuit packs light, and after holding the push-button for approximately 2 seconds did the LED Display on the SYSCTL circuit pack faceplate cycle through the numbers for the software release?

If...	Then...
Yes,	Continue with the next step.
No,	Go to Step 6.

5 Attempt to establish communications with the network element. Was the attempt to log in to the network element successful?

If...	Then...
Yes,	**STOP! End of Procedure.**
No,	Continue with the next step.

Reference: Procedure 6-26: "Establish communications with Network Element" (p. 6-289)

6 Not touching the bottom latch, slowly lift the top latch of the SYSCTL circuit pack until an *F* appears in the LED Display on the SYSCTL circuit pack faceplate. When the *F* appears immediately close the top latch.

Result: The network element should perform a reset.

7 When the reset is complete, attempt to establish communications with the network element. Was the attempt to log in to the network element successful?

If...	Then...
Yes,	**STOP! End of Procedure.**
No,	Continue with the next step.

Reference: Procedure 6-26: "Establish communications with Network Element" (p. 6-289)

8 **Important!** Continuing this procedure will result in the loss of some provisioning data (for example, logins and passwords, TCP/IP provisioning) stored on the SYSCTL circuit pack. See the *Alcatel-Lucent 1665 Data Multiplexer (DMX) TL1 Message Details, 365-372-306* for a complete list of provisioning data that will be lost.

Not touching the bottom latch, slowly lift the top latch of the SYSCTL circuit pack until an *F* appears in the LED Display on the SYSCTL circuit pack faceplate. When the *F* appears immediately close the top latch

Result: The network element should perform a reset.

9 **Important!** Watch the **CR** LED closely on the SYSCTL circuit pack faceplate. The **CR** LED flashes for 10 seconds only.

When the **CR** LED flashes on the SYSCTL circuit pack faceplate, press the **UPD/INIT** push-button once on the SYSCTL circuit pack.

Important! The **UPD/INIT** push-button is recessed and requires a tool to press it.

Result: The network element should perform another reset.

10 **Important!** The network element logins and passwords have been reset. Use a default network element user ID (for example, LUC01) and password (DMX2.5G10G) when attempting to log in to the network element.

When the reset is complete, attempt to establish communications with the network element. Was the attempt to log in to the network element successful?

If...	Then...
Yes,	**STOP! End of Procedure.**
No,	Continue with the next step.

Reference: Procedure 6-26: "Establish communications with Network Element" (p. 6-289)

11 Remove and reseat the SYSCTL circuit pack.

Result: The network element should perform a reset.

12 **Important!** The network element logins and passwords have been reset. Use a default network element user ID (for example, LUC01) and password (DMX2.5G10G) when attempting to log in to the network element.

When the reset is complete, attempt to establish communications with the network element. Was the attempt to log in to the network element successful?

If...	Then...
Yes,	**STOP! End of Procedure.**
No,	Continue with the next step.

Reference: Procedure 6-26: "Establish communications with Network Element" (p. 6-289)

13 Replace the SYSCTL circuit pack.

Reference: Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99)

14 **Important!** The network element logins and passwords have been reset. Use a default network element user ID (for example, LUC01) and password (DMX2.5G10G) when attempting to log in to the network element.

Attempt to establish communications with the network element. Was the attempt to log in to the network element successful?

If...	Then...
Yes,	**STOP! End of Procedure.**
No,	Contact your next level of support.

Reference: Procedure 6-26: "Establish communications with Network Element" (p. 6-289)

END OF STEPS

Procedure 5-2: Clear "−48V power/fuse FA or FB failed" alarm

Overview

This procedure is used to clear a `−48V power/fuse failed` alarm. The alarm list identifies which power source is affected, either A or B.

Required equipment

In addition to the equipment listed in "Required equipment" (p. 5-7), a power meter is also required.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to identify and clear a `−48V power/fuse failed` alarm.

1 Are both of the power indicators lit on the top of the Alcatel-Lucent 1665 DMX shelf (**BRK A 20A ON** and **BRK B 20A ON**) or the Alcatel-Lucent 1665 DMX High Capacity Shelf (**BRK A 30A ON** and **BRK B 30A ON** or **BRK A 20A ON** and **BRK B 20A ON**)?

If...	Then...
Yes	Proceed to Step 19.
No	Continue with Step 2.

2 Perform a thorough visual inspection of the shelf backplane and side-mounted power connectors. Look for signs of damage or a loose power connection.

Important! Each -48V power feeder supplies redundant power to the shelf circuit packs. It is highly unlikely that a circuit pack failure would cause a circuit breaker to trip. The more probable cause of a failure in a feeder/circuit breaker is a short in the backplane feeder path or a problem with a circuit pack connector.

3 Were any problems found involving the power connections?

If...	Then...
Yes	Broken or shorted power line: repair the short or break, or replace the shelf, as appropriate. Loose power connection: reseat and secure the connector.
No	Continue with Step 4.

4 Monitor the DC power supplied to the shelf.

Important! A -48 VDC power alarm indicates the loss one of the two redundant -48 VDC power feeds.

5 Is the DC voltage normal (-48 VDC) at both connectors?

If...	Then...
Yes	Continue with Step 6.
No	Check the DC power distribution lines supplying power to the shelf.

6 Unseat the SYSCTL circuit pack from the shelf and reset the tripped circuit breaker.

7 Does the circuit breaker remain reset?

If...	Then...
Yes	Return the removed SYSCTL circuit pack for repair. Replace the SYSCTL with a spare. Refer to Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99). **Important!** After replacing the SYSCTL circuit pack, you must log back into the *WaveStar*® CIT. Refer to Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27).

If...	Then...
No	Reinstall the removed circuit pack and proceed to the next circuit pack. **Important!** After replacing the SYSCTL circuit pack, you must log back into the *WaveStar®* CIT. Refer to Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27).

8

NOTICE

Service-disruption hazard

Removing a transmission circuit pack may disrupt service.

Before removing a transmission circuit pack, verify that the circuit pack is not carrying service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Remove the protection circuit packs on the shelf, one at a time. After each removal, reset the tripped circuit breaker.

9 Does the circuit breaker remain reset?

If...	Then...
Yes	Return the removed circuit pack for repair.
No	Reinstall the removed circuit pack and proceed to the next circuit pack.

10

NOTICE

Service-disruption hazard

Removing a transmission circuit pack may disrupt service.

Before removing a transmission circuit pack, verify that the circuit pack is not carrying service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

For the electrical interface transmission circuit packs where protection circuit packs are available, switch the service to the protection circuit pack by selecting select **Fault** → **Protection Switch** from the System View.

11 Highlight the Pack x for the circuit pack that you are removing and click **Select**.

Result: On the right side of the Switch Protection window, the Switch Type: pull-down menu appears.

12 From the Switch Type: pull-down menu, select **Forced** and click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes**.

13 To verify that the switch has occurred:

1. From the System View, select **View** → **Protection**.
2. Highlight the circuit pack that you are replacing and click **Select**.
3. Verify that Protection Switch State: reads Standby and the Equipment State: reads Out of Service.
4. Verify that Protection Switch Priority: reads Forced.

14 Replace the service circuit packs (now Out of Service) one at a time. After each removal, reset the tripped circuit breaker.

15 Does the circuit breaker remain reset?

If...	Then...
Yes	Return the removed circuit pack for repair.
No	Reinstall the removed circuit pack and proceed to the next circuit pack.

16 From the System View, select **Fault** → **Protection Switch**, highlight the appropriate Protection Group, and then click **Select**.

17 In the Protection Switch Mode section of the window, click on the drop down menu for Switch Type. Select **Reset** and click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes**.

18 In the *Switch Protection* window, click **Close**.

19 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `−48V power/fuse failed` alarm is no longer present.

END OF STEPS

Procedure 5-3: Clear "AGNE communication failure" alarm

Overview

This procedure is used to clear an `AGNE communication failure` alarm.

Before you begin

Prior to performing this procedure, refer to “Required equipment” (p. 5-7) and “Before you begin” (p. 5-7) in this chapter.

Steps

Complete the following steps to identify and clear an `AGNE communication failure` alarm.

1 From the *WaveStar®* CIT System View, select **Administration** → **View NE Administration**, to check the provisioning of the AGNE for that NE's alarm group.

Result: The *View NE Administration* window opens.

2 Is the local NE the alarm gateway network element (AGNE)? Alarm Gateway: ENABLED.

If...	Then...
Yes	There is a provisioned AGNE for the alarm group. Proceed to Step 4.
No	Continue with Step 3.

3 Can you determine the AGNE for the alarm group?

If...	Then...
Yes	Record the TID and log into that NE and select **Administration** → **View NE Administration**. Continue with Step 4.
No	Proceed to Step 7.

4 Is Remote NE status enabled for the AGNE?

If...	Then...
Yes	Continue with Step 5.
No	Proceed to Step 7.

5 Log into each NE in the alarm group and select **Administration** → **View NE Administration** from the System View.

6 Is Remote NE status enabled?

If...	Then...
Yes	Repeat Step 5 and Step 6 for each NE in the alarm group. Proceed to Step 13.
No	Continue with Step 7.

7 From the System View, select **Administration** → **Set NE**.

Result: The *Set NE* window opens.

8 For Remote NE Status, select **Enabled** to enable Remote NE Status.

Important! Note that Remote NE Status must be Enabled in order to provision the alarm group functions.

9 For Alarm Gateway, select **Enabled** to provision one NE in the alarm group as the alarm gateway network element (AGNE). Otherwise, select **No**.

10 Enter or select the Alarm Group number (1–255) being assigned to the alarm group for this NE.

Important! The Alarm Group number must be the same for all NEs in that alarm group.

11 Ensure the other parameters in the window have not been changed, unless you are provisioning them also. Click **OK** at the bottom of the window.

12 Read the warning message, then click **Yes** to execute the command.

Important! An `AGNE communication failure` alarm may occur if an AGNE has not yet been provisioned for the alarm group. If you need to clear the alarm, select **Administration** → **Set NE**, then select **Disabled** to disable the Remote NE Status. You will have to enable the remote NE status again once the AGNE has been established in order for this NE to be part of the alarm group.

13 From the *WaveStar®* CIT System View, click the **Alarm List** button and click **Refresh**.

Result: The `AGNE communication failure` alarm is no longer present.

END OF STEPS

Procedure 5-4: Clear "audit failed" alarms

Overview

Use this procedure to clear the following alarms:

- `NP audit failed`
- `Segment audit failed LAN in`
- `Segment audit failed LAN out`
- `Segment audit failed VCG in`
- `Segment audit failed VCG out`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `audit failed` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `audit failed` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Perform the following to remove the affected circuit pack completely from the shelf and then re-seat the circuit pack.

1. Release both circuit pack latches.
2. Remove the circuit pack from the shelf, fully disconnecting it from the backplane and removing power. The **ACTIVE** and **FAULT** LEDs extinguish.
3. Re-seat the circuit pack in the shelf and wait approximately 5 minutes.

4 From the System View, click the **Alarm List** button and click **Refresh**.

5 Is the `audit failed` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

6 Replace the affected circuit pack.

Reference: Procedure 6-7: "Replace Ethernet/Data circuit pack" (p. 6-68)

7 From the System View, click the **Alarm List** button and click **Refresh**.

8 Is the `NP audit failed` alarm still present?

If...	Then...
Yes	Remove the replacement circuit pack and return the original circuit pack to the slot, then continue with the next step.
No	STOP! End of Procedure.

9 **Important!** The `NP audit failed` alarm can also be caused by excessive broadcast type Ethernet frames running through the network processor. The maximum through capacity of the LNW70/170 circuit pack is 9 Gigabits.

Using local procedures, customers should alter their network traffic patterns to reduce the amount of broadcast/multicast traffic being sent to the affected circuit pack.

10 From the System View, click the **Alarm List** button and click **Refresh**.

If the `audit failed` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-5: Clear "AUTO link shutdown" alarm

Overview

This procedure is used to clear an `AUTO link shutdown` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `AUTO link shutdown` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `AUTO link shutdown` alarm in the resulting alarm list.

2 **Important!** The `AUTO link shutdown` alarm is reported when the local network element detects a remote client signal fail message from the far-end network element or a VCG failure occurs and the local port Remote Client Fail Link Shutdown parameter is Enabled.

Important! For FE and GE ports on the LNW63, LNW64, LNW74, LNW87, and LNW70/LNW170 packs, the `AUTO link shutdown` alarm is also reported when the local network element detects a remote GFP RDI message from the far-end network element and both the local port Remote Client Fail Reverse Defect Indication and the local port Remote Client Fail Link Shutdown parameters are enabled.

Remote GFP RDI messages are received when the far-end network element has a VCG failure while the Remote Client Fail Reverse Defect Indication and the Remote Client Fail parameters are enabled.

Locate and clear all `Remote client signal failed` and `inc. VCG failed` alarms in the alarm list.

Reference:

- Procedure 5-75: "Clear "inc. VCG failed" alarm" (p. 5-199)
- Procedure 5-118: "Clear "Remote client signal failed" alarm" (p. 5-292)

3 From the System View, click the **Alarm List** button and click **Refresh**.

If the `AUTO link shutdown` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-6: Clear "automatic lock" condition

Overview

This procedure is used to clear an `automatic lock` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `automatic lock` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `automatic lock` condition in the resulting alarm list and note the corresponding AID.

2 Look for equipment alarms/conditions affecting the same AID. Proceed to the appropriate procedure to clear those alarms/conditions.

3 From the System View, select **View** → **Equipment**, highlight DMX, click **Select**.

Result: The *View Equipment* window opens.

4 Record the AutoLock information.

Important! Count is the number of equipment switches that occurred during the Switch Interval. Switch Interval and Release Interval are in minutes. The defaults are 25 and 1440 (24 hours), respectively.

Count:	
Switch Interval:	
Release Interval:	

5 The `automatic lock` condition will clear automatically when the provisioned Release Interval (Step 4) passes. Do you wish to wait the indicated number of minutes for the condition to clear?

If...	Then...
Yes	Proceed to Step 12.
No	Continue with Step 6.

6 Does the AID indicate the mains (main-1 or main-2) or a DS3 equipment pair?

If...	Then...
Main	Proceed to Step 10.
DS3	Continue with Step 7.

7 From the System View, select **Fault** → **Protection Switch**, highlight the appropriate Protection Group and then click **Select**.

Result: The *Switch Protection* window opens.

8 In the Protection Switch Mode section of the window, click on the drop down menu for Switch Type. Select **Reset** and click **Apply**.

Important! You can also select either Inhibit or **Forced** (each a higher priority request than autolock) to clear the automatic lock condition. However, **Inhibit** and **Forced** also result in a Standing Condition (SC) in the *WaveStar*® CIT Alarm List.

Result: A warning message appears asking you to confirm executing this command. Click **Yes**.

9 In the *Switch Protection* window, click **Close**. Then proceed to Step 12.

10 From the System View, select **Fault** → **Timing/Sync Protection Switch** → **Main Circuit Pack Timing Switch**.

Result: The *Switch Main Circuit Pack Timing* window opens.

11 In the Main Circuit Pack Timing Switch screen, click on the drop down menu for Switch Command. Select **Reset** and click **OK**.

Result: Confirmation message appears. Click **Yes**.

12 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `automatic lock` condition is no longer present.

END OF STEPS

Procedure 5-7: Clear "Automatic protection switch mode mismatch" alarm

Overview

This procedure is used to clear an `Automatic protection switch mode mismatch` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `Automatic protection switch mode mismatch` alarm.

---

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `Automatic protection switch mode mismatch` alarm in the resulting alarm list and note the corresponding AID.

---

2 Refer to office records to determine the correct provisioning for the port *Application* parameter of the applicable optical port pair. (The port *Application* parameter of the applicable local optical port pair is currently provisioned Bidirectional 1+1 or Optimized 1+1.)

---

3 To clear the `Automatic protection switch mode mismatch` alarm either change the port Application parameter of the applicable local port pair or change the port Application parameter of the applicable far-end port pair according to office records and local procedures.

If changing the port Application parameter of the...	Then...
far-end optical port pair,	notify personnel at the site supplying the optical signal to change the port Application parameter according to office records and go to Step 6.

If changing the port Application parameter of the...	Then...
local optical port pair,	go to the next step.

4 From the System View, select **Configuration** → **Equipment**. Expand the required circuit pack. Select the required port and click **Select**.

Result: The port provisionable parameters appear.

5 Provision the port *Application* parameter according to office records and click **Apply** and **Close**.

6 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `Automatic protection switch mode mismatch` alarm is no longer present.

END OF STEPS

Procedure 5-8: Clear "Automatic protection switch primary section mismatch" alarm

Overview

This procedure is used to clear an `Automatic protection switch primary section mismatch` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `Automatic protection switch primary section mismatch` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Automatic protection switch primary section mismatch` alarm in the resulting alarm list and note the corresponding AID.

2 Are there any `inc. OCN` alarms present in the alarm list?

If...	Then...
Yes	Proceed to the appropriate procedure to clear each alarm in order of severity. Continue with Step 3.
No	Proceed to Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `Automatic protection switch primary section mismatch` alarm still present?

If...	Then...
Yes	Continue with Step 5.
No	STOP! End of Procedure.

5 At both the near-end and far-end network elements, select **Fault** → **Protection Switch** to access the required Optimized 1+1 protection group and perform a *Switch Type:* **Reset**.

6 From the System View, click the **Alarm List** button and click **Refresh**.

7 Is the `Automatic protection switch primary section mismatch` alarm still present?

If...	Then...
Yes	Continue with Step 8.
No	STOP! End of Procedure.

8 From the System View, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

9 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

10 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

11 Log back into the network element. Click the **Alarm List** button and click **Refresh**.

12 Is the `Automatic protection switch primary section mismatch` alarm still present?

If...	**Then...**
Yes	Contact your next level of support.
No	STOP! End of Procedure.

END OF STEPS

Procedure 5-9: Clear "Automatic protection switch unused codes" alarm

Overview

This procedure is used to clear an `Automatic protection switch unused codes` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `Automatic protection switch unused codes` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `Automatic protection switch unused codes` alarm in the resulting alarm list and note the corresponding AID.

2 Refer to office records to determine the correct provisioning for the port *Application* parameter of the applicable optical port pair. (The port *Application* parameter of the applicable local optical port pair is currently provisioned Optimized 1+1.)

3 To clear the `Automatic protection switch unused codes` alarm either change the port Application parameter of the applicable local port pair or change the port Application parameter of the applicable far-end port pair according to office records and local procedures.

If changing the port Application parameter of the...	Then...
far-end optical port pair,	notify personnel at the site supplying the optical signal to change the port Application parameter according to office records and go to Step 6.
local optical port pair,	go to the next step.

4 From the System View, select **Configuration** → **Equipment**. Expand the required circuit pack. Select the required port and click **Select**.

Result: The port provisionable parameters appear.

5 Provision the port *Application* parameter according to office records and click **Apply** and **Close**.

6 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `Automatic protection switch unused codes` alarm is no longer present.

END OF STEPS

Procedure 5-10: Clear "Automatic protection switch unresolved transient codes" alarm

Overview

This procedure is used to clear an `Automatic protection switch unresolved transient codes` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `Automatic protection switch unresolved transient codes` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Automatic protection switch unresolved transient codes` alarm in the resulting alarm list and note the corresponding AID.

2 **Important!** The `Automatic protection switch unresolved transient codes` alarm is reported when a System Controller reset or protection switch lockout is performed at the far-end network element disabling protection switching. If a System Controller reset has been performed, protection switching is disabled until the System Controller recovers. If a protection switch lockout has been performed, protection switching is disabled until a protection switch Reset is performed.

Contact personnel at the far-end site supplying the optical signal according to local procedures.

If...	Then...
a lockout is in effect for the applicable protection group at the far-end site,	notify personnel at the far-end site to clear any lockout requests according to local procedures and go to the next step.
a reset is in progress at the far-end site,	wait until the reset is complete and go to the next step.

3 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `Automatic protection switch unresolved transient codes` alarm is no longer present.

END OF STEPS

Procedure 5-11: Clear "inc. BDI" alarms

Overview

This procedure is used to clear the following alarms:

- `inc. ODU2 BDI`
- `inc. OTU2 BDI`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. BDI` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `inc. BDI` alarm in the resulting alarm list.

2 **Important!** The `inc. BDI` alarm indicates that the far-end network element has detected a bad ODU2/OTU2 signal from this network element. The trouble is in the local network element or in the fiber/cable between the local network element and the far-end network element. The `inc. BDI` alarm is normally cleared by addressing other alarms/conditions.

Are there other circuit pack/pluggable transmission module/ODU2/OTU2-related conditions/alarms in the alarm list?

If...	Then...
Yes	Proceed to the appropriate procedures to clear the alarms in order of severity. Then continue with the next step.
No	Proceed to Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `inc. BDI` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

5 Visually check the local transmit fiber connections between the XM10G/8 circuit pack faceplate/pluggable transmission module and the OMD circuit pack faceplate (if equipped), LGX panel, or equivalent connection point for faulty connections or damage.

If faulty connections or damage was...	Then...
found,	Follow local procedures to repair/replace as necessary. Then continue with the next step.
not found,	Proceed to Step 8.

6 From the System View, click the **Alarm List** button and click **Refresh**.

7 Is the `inc. BDI` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

8 Select **View** → **OCH Cross-Connections** to obtain the current list of OCH cross-connections for the required XM10G/8 circuit pack. Verify that the correct OCH cross-connections have been provisioned using office records.

If the correct OCH cross-connections...	Then...
have been provisioned,	Proceed to Step 11.

If the correct OCH cross-connections...	Then...
have *not* been provisioned,	Select **Configuration** → **OCH Cross-Connections** to access the *OCH Cross-Connection Wizard* and provision the required OCH cross-connections. Then continue with the next step.

9 From the System View, click the **Alarm List** button and click **Refresh**.

10 Is the `inc. BDI` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

11 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local pluggable transmission module.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

12 From the System View, click the **Alarm List** button and click **Refresh**.

13 Is the `inc. BDI` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.

If...	Then...
No	STOP! End of Procedure.

14 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local XM10G/8 circuit pack.

Reference: Procedure 6-29: "Replace 10G Muxponder circuit pack" (p. 6-296)

15 From the System View, click the **Alarm List** button and click **Refresh**.

16 Is the `inc. BDI` alarm still present?

If...	Then...
Yes	Remove the replacement XM10G/8 circuit pack and return the original circuit pack to the slot, then continue with the next step.
No	STOP! End of Procedure.

17 **Important!** At this point, the local network element is operating correctly. The trouble is in the far-end network element or in the fiber/cable between the far-end network element and the local network element.

Follow local procedures for addressing conditions/alarms at the far-end network element.

18 From the System View, click the **Alarm List** button and click **Refresh**.

19 Is the `inc. BDI` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

20 Follow local procedures to isolate and clear the fiber/cable trouble between the far-end network element and the local network element.

END OF STEPS

Procedure 5-12: Clear "Circuit Provisioning Error" alarm

Overview

This procedure is used to clear a `Circuit Provisioning Error` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to identify and clear a `Circuit Provisioning Error` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Circuit Provisioning Error` alarm in the resulting alarm list and note the corresponding AID.

2 From the System View, select **View** → **Rings** → **Circuit**.

Result: The *View Circuit* window opens.

3 In the *View Circuit* window, locate the incorrectly provisioned source or destination (loca/locz) at some point in the circuit and record the TID of that node. Click **Close** on the *View Circuit* window.

4 Log in to the NE with the incorrectly provisioned source or destination (loca/locz).

5 From the System View, select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and modify the existing cross-connection.

END OF STEPS

Procedure 5-13: Clear "CP failed/CP contributing to a pack failure" alarms

Overview

This procedure is used to clear the following alarms:

- `DATA CP failed`
- `DS1 CP failed`
- `DS1E1 CP failed`
- `DS3EC1 CP failed`
- `FE-LAN CP failed`
- `GE-LAN CP failed`
- `Muxponder CP failed`
- `OLIU CP failed`
- `OMD CP failed`
- `SWITCH CP failed`
- `SYSCTL CP failed`
- `TMUX CP failed`.

Important! The `CP failed` alarms may be reported with one or more `CP contributing to a pack failure` alarms. The `CP contributing to a pack failure` alarms identify additional circuit packs that have contributed to the failed circuit pack. The `CP failed` alarms must be addressed before the `CP contributing to a pack failure` alarms.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `CP failed` alarm and any associated `CP contributing to a pack failure` alarms.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `CP failed` alarm and any `CP contributing to a pack failure` alarms in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID for the `CP failed` alarm.

3

If the affected circuit pack is ...	Then
All OCN OLIUs except LNW59 OC-192, LNW55 OC3/OC12/OC48, LNW62 4OC-48, LNW82 OC3/OC12/OC48, LNW504 OC-48/OC-192, and LNW603 OC-192 SWITCH SYSCTL	Proceed to Step 7.
LNW59 OC-192 LNW55 OC3/OC12/OC48 LNW62 4OC-48 LNW82 OC3/OC12/OC48 LNW504 OC-48/OC-192 LNW603 OC-192 DATA DS1 DS1E1 DS3/EC1 Fast Ethernet Gigabit Ethernet XM10G/8 OMD TMUX	Continue with the next step.

4 From the System View, select **Fault** → **Reset** → **Smart Pack**. Select the required circuit pack and click **Select**. Click **Apply** to reset the circuit pack.

Result: A warning may appear asking you to confirm executing this command. Click **Yes** to reset the smart circuit pack. A dialog box appears indicating a successful reset. Click **OK**.

A smart pack reset may take several minutes to complete depending on the circuit pack type.

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `CP failed` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

7 From the System View, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

8 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

9 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

10 Log back into the network element. Click the **Alarm List** button and click **Refresh**.

11 Is the `CP failed` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

12 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Perform the following to remove the affected circuit pack completely from the shelf and then re-seat the circuit pack.

1. Release both circuit pack latches.
2. Remove the circuit pack from the shelf, fully disconnecting it from the backplane and removing power. The **ACTIVE** and **FAULT** LEDs extinguish.
3. Re-seat the circuit pack in the shelf and wait approximately 5 minutes.

13 From the System View, click the **Alarm List** button and click **Refresh**.

14 Is the `CP failed` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

15 Replace the affected circuit pack.

Reference: Refer to the appropriate circuit pack replacement procedure in Chapter 6, “Supporting procedures”.

16 From the System View, click the **Alarm List** button and click **Refresh**.

17 Is the `CP failed` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

18 Is a `CP contributing to a pack failure` alarm present in the alarm list?

If...	Then...
Yes	Refer to the Probable Cause column in the alarm list and note the corresponding AID. Then repeat Step 3 through Step 17 for each affected circuit pack. Then continue with the next step.
No	Proceed to Step 21.

19 From the System View, click the **Alarm List** button and click **Refresh**.

20 Is the `CP failed` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

21 Replace the SYSCTL circuit pack.

Reference: Procedure 6-10: “Upgrade or replace SYSCTL (LNW2) circuit pack” (p. 6-99)

22 From the System View, click the **Alarm List** button and click **Refresh**.

23 Is the `CP failed` alarm still present?

If...	Then...
Yes	Contact your next level of support.
No	STOP! End of Procedure.

END OF STEPS

Procedure 5-14: Clear "CP not allowed - crs" alarm

Overview

This procedure is used to clear a `CP not allowed - crs` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `CP not allowed - crs` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `CP not allowed - crs` alarm in the resulting alarm list.

2 Determine the alarm level(s) for the active `CP not allowed - crs` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding slot AID.

4 Select **Reports** → **Equipment Lists** → **Pack**. Click *Shelf* and **Select** to obtain the *Circuit Pack List*. Observe the correct circuit pack information for the required slot.

5 Compare the correct circuit pack information from the *Circuit Pack List* with the circuit pack that is physically in the required slot.

If the circuit packs...	Then...
are the same type,	Perform the following: 1. Select **View** → **Cross-Connections**. Select the required circuit pack and click **Select** to obtain a list of cross-connections. Observe the provisioned cross-connections for the required circuit pack and compare with office records. 2. Select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and make the required cross-connections changes to/from the circuit pack.
are *not* the same type,	Perform the following: 1. Obtain the correct type of circuit pack (according to the *Circuit Pack List*) for the required slot. 2. Replace the wrong circuit pack currently in the required slot with the correct circuit pack. Refer to the appropriate circuit pack replacement procedure in Chapter 6, “Supporting procedures”.

END OF STEPS

Procedure 5-15: Clear "CP not allowed - eqpt" alarm

Overview

This procedure is used to clear a `CP not allowed - eqpt` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Laser safety” (p. 1-6) and “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear a `CP not allowed - eqpt` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `CP not allowed - eqpt` alarm in the resulting alarm list.

2 Determine the alarm level(s) for the active `CP not allowed - eqpt` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding slot AID.

4 Using office records, determine the correct circuit pack type for the required slot.

5 From the System View, select **Reports** → **Equipment Lists** → **Pack**. Select *Shelf* and click **Select** to obtain the *Circuit Pack List*. Observe the circuit pack information for the required slot.

6 Compare the correct circuit pack information from office records with the circuit pack information from the *Circuit Pack List* and the circuit pack that is physically in the required slot.

7 Is the correct circuit pack physically installed in the required slot?

If ...	Then...
Yes,	Select **Configuration** → **Update System** → **Update Inventory**. A dialog box appears asking you to confirm executing this command. Click **Yes**.
No,	Perform the following: 1. Obtain the correct type of circuit pack (according to office records and the *Circuit Pack List*) for the required slot. 2. Replace the wrong circuit pack currently in the required slot with the correct circuit pack. Refer to the appropriate circuit pack replacement procedure in Chapter 6, "Supporting procedures".

END OF STEPS

Procedure 5-16: Clear "CP removed or CP failure" alarm

Overview

This procedure is used to clear a `CP removed or CP failure` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `CP removed or CP failure` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `CP removed or CP failure` alarm in the resulting alarm list.

2 Determine the alarm level(s) for the active `CP removed or CP failure` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list and note the corresponding slot AID.

4 **Important!** The `CP removed or CP failure` alarm is reported when a circuit pack is removed from a slot or when a slot is equipped with a circuit pack that has a failed power module.

Locate the required slot and determine if a circuit pack is physically present in the required slot.

5 Is a circuit pack physically present in the required slot?

If...	Then...
Yes,	Replace the failed circuit pack in the required slot. Refer to the appropriate circuit pack replacement procedure in Chapter 6, "Supporting procedures". STOP! End of Procedure.
No,	Continue with Step 6.

6 Using office records, determine if the required slot should contain a circuit pack.

7 Do office records show that the required slot should contain a circuit pack?

If...	Then...
Yes,	Obtain the missing circuit pack and install it into the required slot. Refer to the appropriate circuit pack installation procedure in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.
No,	Select **Configuration** → **Update System** → **Update All**. A dialog box appears asking you to confirm executing this command. Click **Yes**. This system update clears all current `CP removed or CP failure` alarms.

END OF STEPS

Procedure 5-17: Clear "CP software upgrade required" condition

Overview

This procedure is used to clear a `CP software upgrade required` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `CP software upgrade required` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the CP software upgrade required alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 Un-seat and then re-seat the alarmed circuit pack.

Result: SYSCTL reinitializes the pack and should automatically update the firmware on the newly installed pack.

4 From the *WaveStar®* CIT System View, click the **Alarm List** and **Refresh** buttons.

5 Is the `CP software upgrade required` alarm still present?

If...	Then...
Yes	Continue with Step 6.
No	STOP! End of Procedure.

6 From the System View, select **Configuration** → **Software** → **Apply Software** to schedule a *Smart* or *Smart, Override Alarms* software apply.

Result: Approximately 15 minutes after the scheduled apply time, the apply is complete. You will be logged off the system when the system resets.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

Reference: Procedure 6-20: "Apply software generic" (p. 6-249)

7 Log back into the shelf.

8 From the *WaveStar*® CIT System View, click the **Alarm List** and **Refresh** buttons.

9 Is the `CP software upgrade required` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

10 From the System View, select **Configuration** → **Software** → **Apply Software** to schedule a Forced software apply.

Result: Approximately 15 minutes after the scheduled Forced apply time, the apply is complete. You will be logged off the system when the system resets.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

Reference: Procedure 6-20: "Apply software generic" (p. 6-249)

11 Log back into the shelf.

12 From the *WaveStar*® CIT System View, click the **Alarm List** and **Refresh** buttons.

If the `CP software upgrade required` alarm is still present, you may need to replace the pack. Contact your next level of support.

END OF STEPS

Procedure 5-18: Clear "DATA terminal loopback" condition

Overview

This procedure is used to clear a `DATA terminal loopback` condition. The condition indicates that a user initiated a Data terminal loopback.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `DATA terminal loopback` condition.

1 From the *WaveStar*® CIT System View, click the Alarm List button and locate the `DATA terminal loopback` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 From the System View, select **Fault** → **Analysis** → **Loopback**, expand the appropriate Data circuit pack, select the required Data port, and click **Select**.

Result: The *Loopback* window opens.

4 From the Loopback window, click **Release** and **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-19: Clear "Default K-bytes" alarm

Overview

This procedure is used to clear a `Default K-bytes` alarm.

Important! When this alarm is present, protection switching at the BLSR node is unavailable.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Default K-bytes` alarm.

1 In the alarm list, are there any `inc. OCN` or `inc. STSN` alarms present?

If...	Then...
Yes	Proceed to the appropriate procedure to clear each alarm in order of severity.
No	Continue with Step 2.

2 **Important!** The port Application parameter of the OC-N ports that interface with the BLSR must be provisioned *2F BLSR*.

At each node in the BLSR, use **View** → **Equipment** to access the required OC-N ports and verify that the port Application parameter is provisioned *2F BLSR*.

If required, use **Configuration** → **Equipment** to access the required OC-N ports and provision the port Application parameter *2F BLSR*.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `Default K-bytes` alarm still present?

If...	**Then...**
Yes	Continue with Step 5.
No	STOP! End of Procedure.

5 From the System View, select **Reports** → **Remote NE Alarm List**.

Result: The *Remote NE Alarm List* window opens.

6 Are there any alarms present at the remote NEs?

If...	**Then...**
Yes	Log in to the remote NE and clear all alarms in order of severity. Continue with Step 7.
No	Continue with Step 9.

7 From the System View, click the **Alarm List** button and click **Refresh**.

8 Is the `Default K-bytes` alarm still present?

If...	**Then...**
Yes	Continue with Step 9.
No	STOP! End of Procedure.

9 From the System View, select **View** → **Ring Map** → **Ring Map**. Select the required ring and click **Select**. Verify that the ring map was provisioned correctly.

Result: The *Ring Map* window opens.

10 Is either the West Link or the East Link Isolated?

If...	Then...
Yes	The adjacent node on the corresponding side (East or West) is either being initialized, powered up, powered down. Wait for the node to come up again.
No	Continue with Step 11.

11 From the System View, click the **Alarm List** button and click **Refresh**.

12 Is the `Default K-bytes` alarm still present?

If...	Then...
Yes	Contact your next level of support.
No	STOP! End of Procedure.

END OF STEPS

Procedure 5-20: Clear "dormant/exec code mismatch" condition

Overview

This procedure is used to clear a `dormant/exec code mismatch` condition.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear a `dormant/exec code mismatch` condition.

1 From the System View, select **Configuration** → **Software** → **Apply Software** to schedule a *Smart* or *Smart, Override Alarms* software apply.

Result: Approximately 15 minutes after the scheduled apply time, the apply is complete. You will be logged off the system when the system resets.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

Reference: Procedure 6-20: “Apply software generic” (p. 6-249)

2 Log back into the shelf.

END OF STEPS

Procedure 5-21: Clear "DS1 loopback (to DSX)" condition

Overview

This procedure is used to clear a `DS1 loopback (to DSX)` condition. The condition indicates that a user initiated a DS1 facility loopback.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `DS1 loopback (to DSX)` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `DS1 loopback (to DSX)` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 From the System View, select **Fault** → **Analysis** → **Loopback**, expand the appropriate circuit pack, expand the appropriate VT Group, select the affected DS1 port, and then click **Select**.

Result: The *Loopback* window opens.

4 From the Loopback screen, select **Facility** and **Release**. Click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-22: Clear "DS1 loopback (to Fiber)" condition

Overview

This procedure is used to clear a `DS1 loopback (to Fiber)` condition. The condition indicates that a user initiated a DS1 terminal loopback.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `DS1 loopback (to Fiber)` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `DS1 loopback (to Fiber)` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 From the System View, select **Fault** → **Analysis** → **Loopback**, expand the appropriate circuit pack, expand the appropriate VT Group, select the affected DS1 port, and click **Select**.

Result: The *Loopback* window opens.

4 From the Loopback screen, select **Terminal** and **Release**. Click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-23: Clear "DS3 loopback (to DSX)" condition

Overview

This procedure is used to clear a `DS3 loopback (to DSX)` condition. The condition indicates that a user initiated a DS3 facility loopback.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `DS3 loopback (to DSX)` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `DS3 loopback (to DSX)` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding AID.

3 From the System View, select **Fault** → **Analysis** → **Loopback**, expand the appropriate circuit pack, select the affected DS3 port, and click **Select**.

Result: The *Loopback* window opens.

4 From the Loopback screen, select **Facility** and **Release**. Click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-24: Clear "DS3 loopback (to Fiber)" condition

Overview

This procedure is used to clear a `DS3 loopback (to Fiber)` condition. The condition indicates that a user initiated a DS3 terminal loopback.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `DS3 loopback (to Fiber)` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `DS3 loopback (to Fiber)` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 From the System View, select **Fault** → **Analysis** → **Loopback**, expand the appropriate circuit pack, select the affected DS3 port, and click **Select**.

Result: The *Loopback* window opens.

4 From the Loopback screen, select **Terminal** and **Release**. Click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-25: Clear "Duplicate Ring Node" alarm

Overview

This procedure is used to clear a `Duplicate Ring Node` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Obtain office records that specify the nodes in the affected BLSR.

Steps

Complete the following steps to clear a `Duplicate Ring Node` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Duplicate Ring Node` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding BLSR protection group AID.

3 From the System View, use **View** → **Ring Map** → **Ring Map** to access the affected BLSR and view the BLSR ring map.

4 Observe the values of *Node ID* and *Network Entity Title* parameters in the BLSR ring map.

5 **Important!** Possible causes of the alarm are:

- More than 16 nodes in the BLSR. BLSRs support up to a maximum of 16 nodes.
- Two or more ring nodes on the same network element are detected on the same BLSR. More than one ring node on the same network element on the same BLSR is not supported.
- The provisioned value of the TID parameter is the same at more than one network element. Each network element must have a unique TID.

Using the BLSR ring map and office records for the BLSR, determine the cause of the alarm and clear the alarm using local procedures.

6 From the System View, click the **Alarm List** button and click **Refresh**.

7 Is the `Duplicate Ring Node` alarm still present?

If...	Then...
Yes	Contact your next level of support.
No	STOP! End of Procedure.

END OF STEPS

Procedure 5-26: Clear "E1 loopback (to DSX)" condition

Overview

This procedure is used to clear an `E1 loopback (to DSX)` condition. The condition indicates that a user initiated a E1 facility loopback.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear a `E1 loopback (to DSX)` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `E1 loopback (to DSX)` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 From the System View, select **Fault** → **Analysis** → **Loopback**, expand the appropriate circuit pack, select the affected E1 port, and click **Select**.

Result: The *Loopback* window opens.

4 From the Loopback screen, select **Facility** and **Release**. Click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-27: Clear "E1 loopback (to Fiber)" condition

Overview

This procedure is used to clear a `E1 loopback (to Fiber)` condition. The condition indicates that a user initiated a E1 terminal loopback.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `E1 loopback (to Fiber)` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `E1 loopback (to Fiber)` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 From the System View, select **Fault** → **Analysis** → **Loopback**, expand the appropriate circuit pack, select the affected E1 port, and click **Select**.

Result: The *Loopback* window opens.

4 From the Loopback screen, select **Terminal** and **Release**. Click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-28: Clear "EC1 loopback (to DSX)" condition

Overview

This procedure is used to clear an `EC1 loopback (to DSX)` condition. The condition indicates that a user initiated an EC-1 facility loopback.

Important! Proper terminating and pass through cross-connections must exist at each shelf (including stand-alone shelves) to establish continuity for the EC-1 circuit being tested.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `EC1 loopback (to DSX)` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `EC1 loopback (to DSX)` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 From the System View, select **Fault** → **Analysis** → **Loopback**, expand the appropriate circuit pack, select the affected EC-1 port, and click **Select**.

Result: The *Loopback* window opens.

4 From the Loopback screen, select **Facility** and **Release**. Click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-29: Clear "EC1 loopback (to Fiber)" condition

Overview

This procedure is used to clear an `EC1 loopback (to Fiber)` condition. The condition indicates that a user initiated an EC-1 terminal loopback.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `EC1 loopback (to Fiber)` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `EC1 loopback (to Fiber)` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 From the System View, select **Fault** → **Analysis** → **Loopback**, expand the appropriate circuit pack, select the affected EC-1 port, and click **Select**.

Result: The *Loopback* window opens.

4 From the Loopback screen, select **Terminal** and **Release**. Click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-30: Clear "ECV - excessive code violation" alarm

Overview

This procedure is used to clear an `ECV - excessive code violation` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Laser safety” (p. 1-6) and “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear an `ECV - excessive code violation` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `ECV - excessive code violation` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected port, and note the corresponding AID.

3

NOTICE

Service-disruption hazard

Disconnecting fibers may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting fibers. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Check the Gigabit Ethernet fibers for loose connections or signs of damage.

4 Was a problem found with the fibers?

If...	Then...
Yes,	Replace any damaged fibers, clean the fiber connectors, and reconnect the fiber to the Gigabit Ethernet circuit pack. Refer to Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151).
No,	Clean the fiber connectors and reconnect the fiber to the Gigabit Ethernet circuit pack. Refer to Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151).

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `ECV - excessive code violation` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

7 **Important!** A likely cause of the alarm is the interfacing customer GELAN equipment creating frames with excessive code violations.

Follow local procedures to clear any alarms/conditions at the interfacing customer GELAN equipment.

8 From the System View, click the **Alarm List** button and click **Refresh**.

9 Is the `ECV - excessive code violation` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

10 From the System View, select **Fault** → **Reset** → **Smart Pack**. Select the required Gigabit Ethernet circuit pack and click **Select**. Click **Apply** to reset the circuit pack.

Result: A warning may appear asking you to confirm executing this command. Click **Yes** to reset the smart circuit pack. A dialog box appears indicating a successful reset. Click **OK**.

A smart pack reset may take several minutes to complete depending on the circuit pack type.

11 From the System View, click the **Alarm List** button and click **Refresh**.

12 Is the `ECV - excessive code violation` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

13 From the System View, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

14 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

15 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

16 Log back into the network element. Click the **Alarm List** button and click **Refresh**.

17 Is the `ECV - excessive code violation` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

18

NOTICE

Service-disruption hazard

Disconnecting fibers and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the Gigabit Ethernet circuit pack.

Reference: Procedure 6-7: "Replace Ethernet/Data circuit pack" (p. 6-68)

19 From the System View, click the **Alarm List** button and click **Refresh**.

20 Is the `ECV - excessive code violation` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

21 **Important!** A likely cause of the alarm is a failure at the interfacing customer GELAN equipment or a problem with cabling/wiring between the local GELAN port and the interfacing customer GELAN equipment.

Follow local procedures to isolate and clear the trouble.

22 From the System View, click the **Alarm List** button and click **Refresh**.

23 Is the `ECV - excessive code violation` alarm still present?

If...	Then...
Yes	Contact your next level of support.
No	STOP! End of Procedure.

END OF STEPS

Procedure 5-31: Clear "ENET loopback" conditions

Overview

This procedure is used to clear the following conditions:

- `ENET facility loopback`
- `ENET terminal loopback`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `ENET loopback` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `ENET loopback` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 From the System View, select **Fault** → **Analysis** → **Loopback** and expand the appropriate Ethernet circuit pack. Select the affected AID and click **Select**.

Result: The *Loopback* window opens.

4 From the Loopback screen, click **Release** and **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-32: Clear "ENNI signaling communication failure with peer" alarm

Overview

This procedure is used to clear a `ENNI signaling communication failure with peer` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `ENNI signaling communication failure with peer` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `ENNI signaling communication failure with peer` alarm in the resulting alarm list and note the corresponding AID.

2 Are SONET and DCC-related alarms present in the alarm list?

If...	Then...
Yes	Proceed to the appropriate procedure to clear each alarm in order of severity. Then continue with the next step.
No	Proceed to Step 5.

3 Click the **Alarm List** button and click **Refresh**.

4 Is the `ENNI signaling communication failure with peer` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

5 From the System View menu, select **Administration** → **Data Communications** and click the *SCN* tab to access the *SCN IP Communications* parameters. Using office records, verify that the *SCN IP Manual IP Route* information is provisioned correctly.

If required, click on the desired edit icon (glasses) to add/modify/delete an entry. If changes were made, click **Apply** and **Close** and continue with the next step; otherwise, click **Close** and proceed to Step 8.

6 Click the **Alarm List** button and click **Refresh**.

7 Is the `ENNI signaling communication failure with peer` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

8 Using office records, identify and log in to the far-end peer network element.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

9 At the far-end peer network element, select **Administration** → **Data Communications** and click the *SCN* tab to access the *SCN IP Communications* parameters. Using office records, verify that the *SCN IP Manual IP Route* information is provisioned correctly.

If required, click on the desired edit icon (glasses) to add/modify/delete an entry. If changes were made, click **Apply** and **Close** and continue with the next step; otherwise, click **Close** and proceed to Step 12.

10 At the local network element, click the **Alarm List** button and click **Refresh**.

11 Is the `ENNI signaling communication failure with peer` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

12 At the local network element, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

13 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

14 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

15 Log back into the local network element. Click the **Alarm List** button and click **Refresh**.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

16 Is the `ENNI signaling communication failure with peer` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

17 At the far-end peer network element, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

18 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

19 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

20 At the local network element, click the **Alarm List** button and click **Refresh**.

If the `ENNI signaling communication failure with peer` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-33: Clear "environmentn" alarm

Overview

This procedure is used to clear an `environmentn` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `environmentn` alarm/condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `environmentn` alarm/condition in the resulting alarm list.

2 Determine the alarm level(s) for the active `environmentn` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

4 From the System View, select **View** → **Misc. Discretes** and expand **Input**.

Result: The *View Miscellaneous Discretes* window opens.

5 Can you clearly identify the cause of the condition?

If...	Then...
Yes	Clear using local procedures. STOP! End of Procedure.
Yes; Environment 15 is fan failure	Proceed to Procedure 5-39: "Clear "fan shelf failed" alarm" (p. 5-95).
No	Contact your next level of support.

END OF STEPS

Procedure 5-34: Clear "ERP - Multiple RPL Owners" alarm

Overview

This procedure is used to clear an `ERP - Multiple RPL Owners` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Obtain office records identifying the nodes in the ring and the correct Ethernet ring protection RPL ID provisioning.

Steps

Complete the following steps to clear an `ERP - Multiple RPL Owners` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `ERP - Multiple RPL Owners` alarm in the resulting alarm list and note the corresponding AID.

2 **Important!** Only one RPL owner node is allowed in the ring.

Using office records determine which node in the ring is the RPL owner node.

3 Log in to each node in the ring one at a time and verify that the *RPL ID* parameter is provisioned correctly.

If the node is a...	Then...
Alcatel-Lucent 1665 DMX	From the System View, select **View** → **Data** → **ERP** and the required Ethernet circuit pack to obtain Ethernet ring protection provisioning. If required, select **Configuration** → **Data** → **Create/Modify/Delete ERP** and the required Ethernet circuit pack/ring to reprovision the RPL ID parameter.

If the node is a...	Then...
another product,	Use product's documentation to log in and obtain the required port/VCG Ethernet ring protection provisioning. If required reprovision the RPL ID parameter.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

END OF STEPS

Procedure 5-35: Clear "ERP - PDU Watchdog Timeout" alarm

Overview

This procedure is used to clear an `ERP - PDU Watchdog Timeout` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Obtain office records identifying the nodes in the ring and the correct Ethernet ring protection provisioning.

Steps

Complete the following steps to clear an `ERP - PDU Watchdog Timeout` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `ERP - PDU Watchdog Timeout` alarm in the resulting alarm list and note the corresponding AID.

2 Using office record determine if this node is the RPL owner node.

If this node is ...	Then...
the RPL owner node,	From the System View, select **Configuration** → **Data** → **Create/Modify/Delete ERP** to access the required Ethernet circuit pack/ring. Disable the *ERP State* parameter, and then Enable the *ERP State* parameter. Proceed to Step 10
a non-RPL owner node,	Continue with the next step.

3 From the System View, select **View** → **Data** → **ERP**. Select the required Ethernet circuit pack and click **Select**.

Result: The ERP information appears.

4 **Important!** The local node may be using the wrong VLAN or MD level.

Compare the provisioned values of the provisionable ERP parameters with office records to verify that the provisioned values are correct.

If the provisionable ERP parameters...	Then...
correct,	Proceed to Step 7.
not correct,	From the System View, select **Configuration** → **Data** → **Create/Modify/Delete ERP** to access the required Ethernet circuit pack/ring and provision the ERP parameters according to office records. Then continue with the next step.

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `ERP - PDU Watchdog Timeout` condition still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

7 **Important!** Only one RPL owner node is required in the ring. There may be *no* RPL Owner node provisioned (or it is disabled).

Using office records determine which node in the ring is the designated RPL owner node.

8 Log in to the designated RPL owner node (according to office records) and verify that the provisionable ERP parameters are provisioned correctly.

If the node is a...	Then...
Alcatel-Lucent 1665 DMX	From the System View, select **View** → **Data** → **ERP** and the required Ethernet circuit pack to obtain Ethernet ring protection provisioning. If required, select **Configuration** → **Data** → **Create/Modify/Delete ERP** and the required Ethernet circuit pack to reprovision the ERP parameters.
another product,	Use product's documentation to log in and obtain the required port/VCG Ethernet ring protection provisioning information. If required reprovision the ERP parameters.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

9 From the System View, click the **Alarm List** button and click **Refresh**.

10 Is the `ERP - PDU Watchdog Timeout` condition still present?

If...	Then...
Yes	Contact your next level of support.
No	STOP! End of Procedure.

END OF STEPS

Procedure 5-36: Clear "Exceeded MTU size drop" alarm

Overview

This procedure is used to clear an `Exceeded MTU size drop` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Obtain office records showing correct provisioning for the affected LAN port/VCG.

Steps

Complete the following steps to clear an `Exceeded MTU size drop` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Exceeded MTU size drop` alarm in the resulting alarm list and note the corresponding AID.

2 From the System View, select **View** → **Equipment**. Expand the required Ethernet circuit pack, select the required port/VCG, and click **Select**.

Result: The port/VCG information appears.

3 Compare the provisioned values of the *MTU Size (in bytes)* and *Exceeded MTU Size Drop Threshold* parameters with office records to verify that the provisioned values are correct.

4

If the provisioned values are...	Then...
correct,	A likely cause of the alarm is a provisioning error or equipment failure in the network. Follow local procedures to isolate and clear the trouble.
not correct,	Select **Configuration** → **Equipment** to access the required port/VCG and reprovision the correct parameter values.

END OF STEPS

Procedure 5-37: Clear "Excessive Reserved Rate on RPR" condition

Overview

This procedure is used to clear an `Excessive Reserved Rate on RPR` condition.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Laser safety” (p. 1-6) and “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear an `Excessive Reserved Rate on RPR` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `Excessive Reserved Rate on RPR` condition in the resulting alarm list and note the corresponding VCG AID.

2 From the System View, select **View** → **Rings** → **Ring Map**. Select the required RPR ring and click **Select**.

Result: The RPR ring map information appears.

3 Observe the *Total Reserved Rate* for the ringlets and the provisioned *Reserved Class A0 Bandwidth* for the local VCG RPR spans.

4 **Important!** The sum of all the provisioned VCG RPR span *Reserved Class A Add Rates* (Mb/s) around the ring has exceeded the link rate of the ring. (The link rate is approximately 48.384 Mb/s per STS-1 cross-connection to the VCG.)

Follow local procedures to either increase the link rate of the ring or decrease the provisioned VCG RPR span *Reserved Class A Add Rate* at one or more nodes in the ring.

If ...	Then ...
increasing the link rate of the ring,	Continue with Step 5.

If ...	Then ...
decreasing the provisioned VCG RPR span *Reserved Class A Add Rate* at one or more nodes in the ring,	Proceed to Step 8.

5 From the System View, select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and provision the additional cross-connection(s) to the required VCGs according to local procedures.

6 **Important!** Each tributary cross-connected to a VCG must be *Enabled* in both the Input and Output Directions before it becomes an active member of the VCG.

From the System View, select **Configuration** → **Equipment**. Expand the required Ethernet circuit pack and VCG details. Select the required tributary being provisioned and click **Select**.

Provision the tributary parameters according to local procedures. Click **Apply**, read the warning message, then click **Yes** to execute the command.

Repeat this step for each tributary being enabled. Click **Close** to exit.

7 At each node in the RPR ring, log in to the node and repeat Step 5 and Step 6 to increase the link rate.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

STOP! End of Procedure.

8 From the System View, select **Configuration** → **Equipment**. Expand the required Ethernet circuit pack, select the required VCG being provisioned, and click **Select**.

Click the **RPR Span** tab and decrease the *Reserved Class A Add Rate (Mb/sec)* according to local procedures. Click **Apply**, read the warning message, then click **Yes** to execute the command.

If required, repeat this step for the other VCG. Click **Close** to exit.

9 If required at other nodes, log in to the node and repeat Step 8 to decrease the provisioned *Reserved Class A Add Rate (Mb/sec)*.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

STOP! End of Procedure.

END OF STEPS

Procedure 5-38: Clear "Extra Traffic Preempted" condition

Overview

This procedure is used to clear an `Extra Traffic Preempted` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `Extra Traffic Preempted` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Extra Traffic Preempted` condition in the resulting alarm list and note the corresponding AID.

2 In the alarm list, are there any `inc. OCN` or `inc. STSN` alarms present?

If...	Then...
Yes	Proceed to the appropriate procedure to clear each alarm in order of severity. Continue with Step 3.
No	Proceed to Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `Extra Traffic Preempted` condition still present?

If...	Then...
Yes	Continue with Step 5.
No	STOP! End of Procedure.

5 In the alarm list, are there any `manual switches` or `forced switches` present?

If...	Then...
Yes	Proceed to the appropriate procedure to clear each alarm in order of severity. Continue with Step 6.
No	Contact your next level of support.

6 From the System View, click the **Alarm List** button and click **Refresh**.

7 Is the `Extra Traffic Preempted` condition still present?

If...	Then...
Yes	Contact your next level of support.
No	STOP! End of Procedure.

END OF STEPS

Procedure 5-39: Clear "fan shelf failed" alarm

Overview

This procedure is used to clear a `fan shelf failed` alarm.

Required equipment

In addition to the equipment listed in "Required equipment" (p. 5-7), the following equipment is also required:

- Small phillips-head screwdriver
- Small flat-blade screwdriver
- Spare Fan Shelf (if necessary)
- Spare Fan Filter (if necessary)
  - For Alcatel-Lucent 1665 DMX comcode: 408 456 770
  - For Alcatel-Lucent 1665 DMX high capacity shelf comcode: 408 682 615

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to isolate and clear a fan failure.

1 Is the power indicator (**PWR ON**) LED lighted on the Alcatel-Lucent 1665 DMX fan shelf?

If...	Then...
Yes	Proceed to Step 4.
No	Continue with the next step.

2 The Fan Shelf has no power. Check power and alarm cables. If cables are not connected, install power and alarm cables to Fan Shelf and tighten screw locks.

3 Is Fan Shelf running and working properly (**PWR ON** LED lighted, **FAULT** LED off, **CLOGGED FILTER** LED off [Alcatel-Lucent 1665 DMX high capacity shelf only])? The Alcatel-Lucent 1665 DMX Fan Shelf needs four fans operating to provide the minimum required airflow.

If...	Then...
Yes	STOP! End of Procedure.
No, **PWR ON** LED *off*,	Proceed to Step 6 to replace the Fan Shelf.
No, **FAULT** LED *lighted* and/or **CLOGGED FILTER** LED *lighted* (Alcatel-Lucent 1665 DMX high capacity shelf only)	Continue with the next step.

4 Replace the fan filter.

Reference: Procedure 6-15: "Replace fan filter" (p. 6-169)

5 Is Fan Shelf running and working properly (**PWR ON** LED lighted, **FAULT** LED off, **CLOGGED FILTER** LED off [Alcatel-Lucent 1665 DMX high capacity shelf only])?

If...	Then...
Yes	STOP! End of Procedure.
No	Continue with Step 6 to replace Fan Shelf.

6 Unscrew the screw locks and disconnect power and alarm cables from fan on the Alcatel-Lucent 1665 DMX shelf or the Alcatel-Lucent 1665 DMX high capacity shelf.

7 Back out the screws securing the fan unit.

Figure 5-1, "Alcatel-Lucent 1665 DMX fan unit screws" (p. 5-97) illustrates the location of the screws on the Alcatel-Lucent 1665 DMX shelf.

Figure 5-1 Alcatel-Lucent 1665 DMX fan unit screws

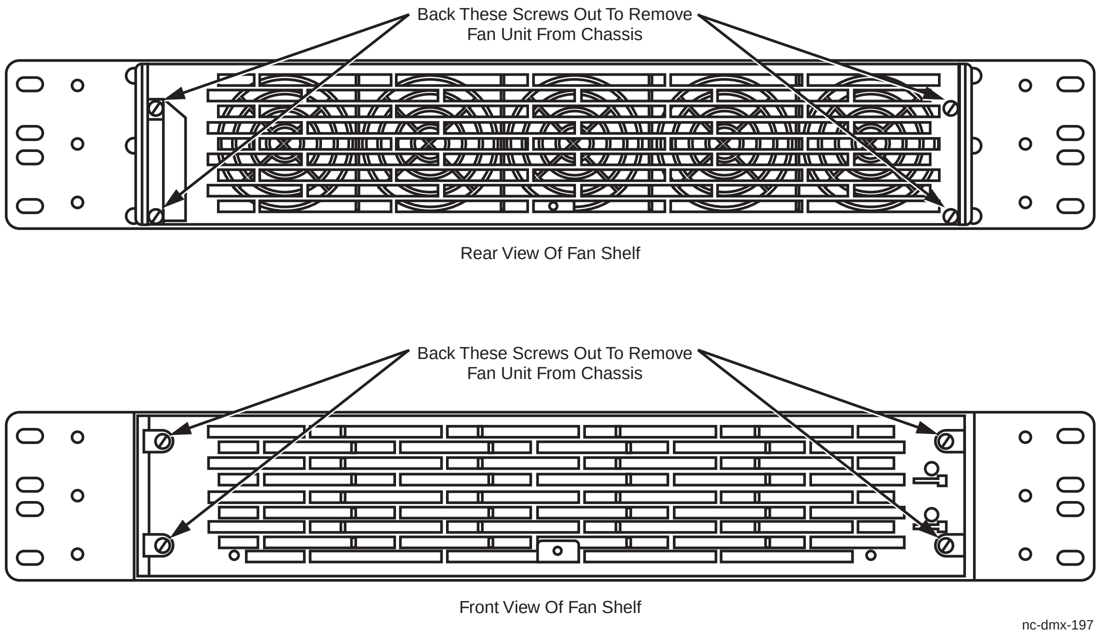
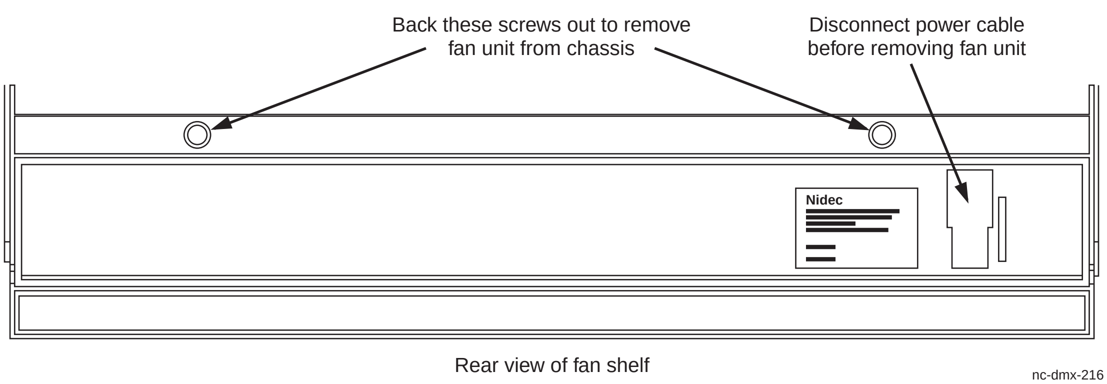


Figure 5-2, "Alcatel-Lucent 1665 DMX High Capacity Shelf fan unit screws" (p. 5-97) illustrates the location of the screws on the Alcatel-Lucent 1665 DMX high capacity shelf.

Figure 5-2 Alcatel-Lucent 1665 DMX High Capacity Shelf fan unit screws



8 Slide the old fan out from the fan chassis.

9 Slide the new fan unit back into the fan chassis. Tighten all screws located in the front and back of the fan unit for the Alcatel-Lucent 1665 DMX shelf or the Alcatel-Lucent 1665 DMX high capacity shelf.

Hand tighten the #4 steel thread fasteners until "snug tight" and then 1/2 turn with a wrench/screwdriver (torque should be approximately 8 in-lb.).

10 Reconnect the power and alarm cables to the back of the fan shelf.

END OF STEPS

Procedure 5-40: Clear "far end not LCAS" condition

Overview

This procedure is used to clear the `far end not LCAS` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `far end not LCAS` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `far end not LCAS` condition in the resulting alarm list and note the corresponding VCG AID.

2 Using circuit layouts and/or office records, identify the far-end network element for the specified VCG.

3 Use the *WaveStar*® CIT to log in to the required far-end Alcatel-Lucent 1665 DMX for the specified VCG.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

4 From the System View, select **Reports** → **Equipment Lists** → **Pack**. Select *Shelf* and click **Select**.

Result: The *Circuit Pack List* appears.

5 **Important!** The LNW63 GBE PL Gigabit Ethernet, LNW70 100/1G-FXS Gigabit Ethernet and LNW74 10/100 Base FX/TX Enhanced Private Line Ethernet circuit packs support LCAS operation.

Using the *Circuit Pack List* and office records, determine if the far-end Alcatel-Lucent 1665 DMX supports LCAS.

6

If the far-end Alcatel-Lucent 1665 DMX...	Then...
supports LCAS and LCAS operation is desired,	go to Step 7 and enable LCAS for the required VCG at the far end.
supports LCAS and LCAS operation is *not* desired,	Disconnect the *WaveStar*® CIT from the far-end Alcatel-Lucent 1665 DMX and go to Step 10 to disable LCAS on the required VCG at the near end (local).
does *not* support LCAS,	Disconnect the *WaveStar*® CIT from the far-end Alcatel-Lucent 1665 DMX and go to Step 10 to disable LCAS on the required VCG at the near end (local).

7 From the System View at the far end, select **Configuration** → **Equipment**. Expand the required Ethernet circuit pack details and select the required VCG port being provisioned. Click **Select**.

8 Select the *LCAS* tab. Provision the LCAS parameters, as required. Click **Apply**.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes**. Click **Close** to exit window.

9 Disconnect the *WaveStar*® CIT from the far-end Alcatel-Lucent 1665 DMX.

STOP! End of Procedure.

10 From the System View at the near end, select **Configuration** → **Equipment**. Expand the required Ethernet circuit pack details and select the required VCG port being provisioned. Click **Select**.

11 Select the *LCAS* tab and disable the LCAS mode. Click **Apply**.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes**. Click **Close** to exit window.

END OF STEPS

Procedure 5-41: Clear "Far-end protection line failure" alarm

Overview

This procedure is used to clear a `Far-end protection line failure` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `Far-end protection line failure` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `Far-end protection line failure` alarm in the resulting alarm list and note the corresponding AID.

2 Contact personnel at the far-end site supplying the optical signal according to local procedures. The condition (trouble) is *not* in the local network element. Notify personnel at the far-end site to clear all alarms.

END OF STEPS

Procedure 5-42: Clear "forced switch" condition

Overview

This procedure is used to clear a `forced switch` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `forced switch` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `forced switch` condition in the resulting alarm list and note the corresponding AID.

2 From the System View, select **Fault** → **Protection Switch**, highlight the affected Protection Group, and then click **Select**.

Result: On the right side of the Switch Protection window, the *Switch Type:* pull-down menu appears.

3 From the *Switch Type:* pull-down menu, select **Reset** and click **Apply**.

Result: A warning message appears asking you to confirm executing this command.

4 Click **Yes** to release the forced switch. Click **Close** to exit the *Switch Protection* window.

END OF STEPS

Procedure 5-43: Clear "Forced Switch" condition

Overview

This procedure is used to clear a `Forced Switch` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Forced Switch` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `forced switch` condition in the resulting alarm list and note the corresponding 2F BLSR protection group AID and direction.

2 From the System View, select **Fault** → **Protection Switch**, highlight the appropriate BLSR Protection Group, and then click **Select**.

Result: On the right side of the Switch Protection window, the *Switch Type:* pull-down menu appears.

3 From the *Switch Type:* pull-down menu, select **Reset** and click **Apply**.

Result: A warning message appears asking you to confirm executing this command.

4 Click **Yes** to release the forced switch. Click **Close** to exit the *Switch Protection* window.

END OF STEPS

Procedure 5-44: Clear "Generic/Database/Equipment Configuration" alarms/conditions

Overview

This procedure is used to clear the following generic, database, and equipment configuration alarms/conditions:

- `Equipment configuration no longer supported`
- `Invalid Database`
- `Maintenance Mode`
- `Multiple Databases`
- `Multiple Generics`

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.
3. Obtain office records specifying the required valid generic.
4. Locate the most recent backup copy of the network element database in case it is necessary to restore the network element database.

Steps

Complete the following steps to clear generic, database, and equipment configuration alarms/conditions.

1 **Important!** When the network element is in the Maintenance Mode state, the **IND** display on the SYSCTL circuit pack faceplate shows *MPx.x* (where *x.x* is the generic number).

If the network element is in the Maintenance Mode state, the default User IDs/passwords must be used to log in to the network element. LUC01, LUC02, and LUC03 are the default privileged User IDs, and DMX2.5G10G is the default privileged password.

Perform the following to log in to the network element using the *WaveStar*® CIT TL1 Cut-Tthrough Mode.

1. From the Network View, log into the NE but this time click **TL1**, not Graphical.
2. Select the *Cut Through Execution Mode* and click **OK**.
3. Enter a default privileged User ID and password. Defaults are **LUC01** and **DMX2.5G10G**, respectively.

   Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) TL1 Message Details, 365-372-306*

2 Execute the **`rtrv-alm-all`** TL1 command to obtain a list of active alarms.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) TL1 Message Details, 365-372-306*

3 Observe the list of active alarms.

If...	Then...
`Invalid Database`, `Multiple Databases`, and/or `Multiple Generics` alarms are listed,	Execute the **`canc-user`** TL1 command to log out of the network element, then proceed to Procedure 5-44.1: “Clear "Generic/Database" alarms” (p. 5-106).
`Equipment configuration no longer supported` alarm is listed,	Execute the **`canc-user`** TL1 command to log out of the network element, then proceed to Procedure 5-44.2: “Clear "Equipment configuration no longer supported" alarm” (p. 5-108).

END OF STEPS

Procedure 5-44.1: Clear "Generic/Database" alarms

Steps

Complete the following steps to clear generic and database alarms.

1 **Important!** When the network element is in the Maintenance Mode state, the **IND** display on the SYSCTL circuit pack faceplate shows *MPx.x* (where *x.x* is the generic number).

If the network element is in the Maintenance Mode state, the default User IDs/passwords must be used to log in to the network element. LUC01, LUC02, and LUC03 are the default privileged User IDs, and DMX2.5G10G is the default privileged password.

Log in to the network element.

Result: The *Maintenance Mode Wizard (Screen 1 of 6)* appears.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

2 Perform the following to choose/download and install the required valid generic, database, and subshelf configuration.

1. Follow the *Maintenance Mode Wizard (Screen 1 of 6)* instructions to set the date and time and click **Next**.
2. Follow the *Maintenance Mode Wizard (Screen 2 of 6)* instructions to choose/download a generic and click **Next**.
3. Follow the *Maintenance Mode Wizard (Screen 3 of 6)* instructions to choose/download a database and click **Next**.
4. Follow the *Maintenance Mode Wizard (Screen 4 of 6)* instructions to use the selected generic and database and click **Next**.
5. Follow the *Maintenance Mode Wizard (Screen 5 of 6)* instructions to choose a subshelf configuration. and click **Next**.
6. Follow the *Maintenance Mode Wizard (Screen 6 of 6)* instructions and verify that the correct generic, database, and subshelf configuration were selected. Then click **Finish**.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

Reference:

- Procedure 6-16: "Ugrade software generic via SFTP" (p. 6-171)
- Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175)
- Procedure 6-18: "Upgrade software generic via FTTD" (p. 6-212)
- Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218)

3 **Important!** If a default database was selected/installed, the default User IDs/passwords must be used to log in to the network element. LUC01, LUC02, and LUC03 are the default privileged User IDs, and DMX2.5G10G is the default privileged password.

If a valid (non-default) database was selected/installed, the provisioned User IDs/passwords may be used to log in to the network element.

When the system reset is complete, log back into the network element.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

4 If a default database was selected/installed, restore the most recent network element database using the **Configuration** → **Software** → **Remote Restore** command, if required.

Reference:

- Procedure 6-21: "Backup and restore NE database via FTP" (p. 6-252)
- Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264)
- Procedure 6-23: "Backup and restore NE database via FTAM" (p. 6-279)

END OF STEPS

Procedure 5-44.2: Clear "Equipment configuration no longer supported" alarm

Steps

NOTICE

Service-disruption hazard

During this procedure a service interruption will occur when the fibers/cable are disconnected.

Service is interrupted until the fibers/cable are reconnected and the traffic is rolled to the replacement circuit pack.

Complete the following steps to clear the `Equipment configuration no longer supported` alarm.

---

1 **Important!** When the network element is in the Maintenance Mode state, the **IND** display on the SYSCTL circuit pack faceplate shows *MPx.x* (where *x.x* is the generic number).

If the network element is in the Maintenance Mode state, the default User IDs/passwords must be used to log in to the network element. LUC01, LUC02, and LUC03 are the default privileged User IDs, and DMX2.5G10G is the default privileged password.

Log in to the network element.

Result: The *Maintenance Mode Wizard (Screen 1 of 6)* appears.

Reference: Procedure 6-2: “Connect Personal Computer (PC) and establish *WaveStar®* CIT session” (p. 6-27)

---

2 Perform the following to choose and install the previous generic and database.

1. Follow the *Maintenance Mode Wizard (Screen 1 of 6)* instructions to set the date and time and click **Next**.
2. Follow the *Maintenance Mode Wizard (Screen 2 of 6)* instructions to choose/download a generic and click **Next**.
3. Follow the *Maintenance Mode Wizard (Screen 3 of 6)* instructions to choose/download a database and click **Next**.
4. Follow the *Maintenance Mode Wizard (Screen 4 of 6)* instructions to use the selected generic and database and click **Next**.

5. Follow the *Maintenance Mode Wizard (Screen 5 of 6)* instructions to choose a subshelf configuration. and click **Next**.
6. Follow the *Maintenance Mode Wizard (Screen 6 of 6)* instructions and verify that the correct generic, database, and subshelf configuration were selected. Then click **Finish**.

   Result: The system resets and you are logged off the system.

   A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

---

3 **Important!** The provisioned User IDs/passwords must be used to log in to the network element.

When the system reset is complete, log back into the network element.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

---

4 **Important!** In Release 7.0.x, LNW66 and LNW71 Ethernet circuit packs are *0x1 compatible* with LNW70 and LNW78 Gigabit Ethernet circuit packs within the same Function/Growth group. In Release 7.1.x, LNW66 and LNW71 Ethernet circuit packs are *0x1 incompatible* with LNW70 and LNW78 Gigabit Ethernet circuit packs within the same Function/Growth group. Therefore, upgrades to Release 7.1.x software are not supported if an LNW66/71 circuit pack and an LNW70/78 circuit pack are in the same Function/Growth group.

Select **Reports** → **Equipment Lists** → **Pack** to obtain the *Circuit Pack List*. Identify the Function/Growth groups that are equipped with an LNW66/71 circuit pack in one slot and an LNW70/78 circuit pack in the other slot.

---

5 **Important!** If a Function/Growth group is equipped with an LNW66/71 circuit pack and an LNW70/78 circuit pack, and the system is to be upgraded with Release 7.1.x software, then one circuit pack must be moved to a different Function/Growth group.

Using local procedures, determine which circuit pack to move to a different Function/Growth group, obtain the required replacement circuit pack/pluggable transmission modules (same circuit pack type), and identify an available slot in another Function/Growth group.

---

6 **Important!** If required, the pluggable transmission modules installed in the original circuit pack may be moved to the replacement circuit pack later in this procedure when the optical fibers are moved.

Install the required replacement circuit pack/pluggable transmission modules (same circuit pack type) in the other available Function/Growth slot. Provision the circuit pack, pluggable transmission modules (if required), ports, VCGs, and virtual switches (if required) according to office records.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*

---

7 **Important!** All cross-connections that are associated with the circuit pack being moved must be identified so that traffic can be moved to the replacement circuit pack (same circuit pack type) in the other available Function/Growth slot.

Select **View** → **Cross-Connections** to access the circuit pack being moved and obtain the current list of cross-connections for the circuit pack. Identify and record all cross-connections to/from the VCGs on the circuit pack being moved. Click **Close** to exit.

---

8 For each 1-way cross-connection identified in Step 7 that adds traffic to a VCG on the circuit pack being moved, select **Configuration** → **Cross-Connections** and use the *Cross-Connection Wizard* to create a cross-connection that bridges traffic from the same source to the required destination VCG on the replacement circuit pack.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*

9

NOTICE

Service-disruption hazard

Removing fiber/cable connections will result in service interruptions. Ensure that you remove only the fiber/cable connections for the circuit pack/port being moved.

It is recommended that a single fiber/cable be moved at a time to minimize service interruptions.

Identify the fiber/cable to be moved. Disconnect the fiber/cable and pluggable transmission module (if required) from the circuit pack.

Result: The system reports an `inc. LOS` alarm for the affected port.

Service is interrupted until the fibers/cable are reconnected and the traffic is rolled to the required VCGs on the replacement circuit pack.

Alarms may also be reported at other nodes in the network.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*

10 Clean all fiber connectors. Connect the transmit/receive fibers/cable and pluggable transmission modules (if required) to the required replacement circuit pack.

Reference:

- Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)
- Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)
- *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*

11 If required, repeat Step 9 and Step 10 to move the remaining fibers/cable to the replacement circuit pack; otherwise, continue with the next step.

12 For each 1-way cross-connection identified in Step 7 that drops traffic from a VCG on the circuit pack being moved, select **Configuration** → **Cross-Connections** and use the *Cross-Connection Wizard* to roll traffic from the existing source VCG to the required source VCG on the replacement circuit pack.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*

13 Select **Configuration** → **Cross-Connections** and use the *Cross-Connection Wizard* to delete the remaining cross-connections to the original VCGs on the circuit pack being moved.

14 Release both latches on the circuit pack being moved and remove the circuit pack from the shelf.

Result: The system reports the `CP removed or CP failure` alarm.

15 Select **Configuration** → **Update System** → **Update All**.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes**.

All alarms clear.

16 **Important!** It is recommended that the network element database be backed up to a remote OS (for example, OMS after an upgrade. This creates a current backup copy that includes the replacement circuit packs. The remote OS could use this backup copy to restore the network element database in the event of a catastrophic failure. Attempts to restore the network element database using a backup copy created prior to the upgrade may result in circuit pack failures.

Back up the network element database using the **Configuration** → **Software** → **Remote Backup** command.

Reference:

- Procedure 6-21: "Backup and restore NE database via FTP" (p. 6-252)
- Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264)
- Procedure 6-23: "Backup and restore NE database via FTAM" (p. 6-279)

17 If required, proceed with applying Release 7.1.0 software.

Reference: Procedure 6-20: "Apply software generic" (p. 6-249)

END OF STEPS

Procedure 5-45: Clear "holdover" conditions/alarms

Overview

This procedure is used to clear the following conditions/alarms:

- `excessive holdover`
- `holdover mode active`.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `holdover`-related conditions/alarms.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button to obtain the alarm list.

2 **Important!** Other alarms/conditions may affect network element synchronization. These alarms/conditions may cause the network element to operate in the synchronization holdover mode.

Are there other synchronization-related alarms/conditions or `inc. OCN` alarms/conditions present?

If...	Then...
Yes	Proceed to the appropriate procedure to clear each alarm/condition in order of severity. Then continue with the next step.
No	Proceed to Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `holdover`-related condition/alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

5 **Important!** The system supports provisionable revertive or nonrevertive synchronization mode switching. If provisioned for nonrevertive mode switching, the system must be manually switched from holdover mode to the provisioned timing mode (external timing or line timing) after a timing reference failure clears.

Select **Fault** → **Timing/Sync Protection Switch** → **Clock Mode Switch**, select **Normal**, and click **OK** to manually switch back to the provisioned timing mode.

END OF STEPS

Procedure 5-46: Clear "illegal CP type" alarm

Overview

This procedure is used to clear an `illegal CP type` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Laser safety” (p. 1-6) and “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear an `illegal CP type` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `illegal CP type` alarm in the resulting alarm list.

2 Determine the alarm level(s) for the active `illegal CP type` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

4 Perform the following to remove the affected circuit pack completely from the shelf and then re-seat the circuit pack.

1. Release both circuit pack latches.
2. Remove the circuit pack from the shelf, fully disconnecting it from the backplane and removing power. The **ACTIVE** and **FAULT** LEDs extinguish.
3. Re-seat the circuit pack in the shelf and wait approximately 5 minutes.

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `illegal CP type` alarm still present?

If...	Then...
Yes	Continue with Step 7.
No	STOP! End of Procedure.

7 From the System View, select **Reports** → **Equipment Lists** → **Pack**, highlight *Shelf*, and click **Select**.

Result: The *Circuit Pack List* appears. Print or Save this list.

8 Verify that the circuit pack in question is supported by the current software generic. If not supported, remove the circuit pack. If desired, replace the circuit pack with a supported circuit pack.

9 From the System View, select **Configuration** → **Update System** → **Update All**.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes**.

10 From the System View, click the **Alarm List** button and click **Refresh**.

If the `illegal CP type` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-47: Clear "Improper APS Codes" alarm

Overview

This procedure is used to clear an `Improper APS Codes` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `Improper APS Codes` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Improper APS Codes` alarm in the resulting alarm list and note the corresponding AID.

2 Are there also incoming signal, pluggable transmission module, or circuit pack-related alarms/conditions associated with that AID?

If...	Then...
Yes	Proceed to the appropriate procedures to clear the alarms in order of severity. Then continue with the next step.
No	Proceed to Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `Improper APS Codes` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

5 Check optical connections for the presence of an incoming signal and measure the optical signal level. Clean the cable ends if needed. If no problem is found, check the line build-outs (LBOs).

Reference: Procedure 6-11: “Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)” (p. 6-151)

6 From the System View, click the **Alarm List** button and click **Refresh**.

7 Is the `Improper APS Codes` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

8 Are the near-end and the far-end OLIU circuit packs equipped with pluggable transmission modules?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 12.

9 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected near-end and then the far-end pluggable transmission module.

Reference: Procedure 6-8: “Replace pluggable transmission module” (p. 6-71)

10 From the System View, click the **Alarm List** button and click **Refresh**.

11 Is the `Improper APS Codes` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

12

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the near-end and then the far-end OC-48 or OC-192 OLIU circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

13 From the System View, click the **Alarm List** button and click **Refresh**.

14 Is the `Improper APS Codes` alarm still present?

If...	Then...
Yes	Remove the replacement OCn circuit pack and return the original circuit pack to the slot, then continue with the next step.
No	STOP! End of Procedure.

15 Replace the SYSCTL circuit pack.

Reference: Procedure 6-10: “Upgrade or replace SYSCTL (LNW2) circuit pack” (p. 6-99)

16 From the System View, click the **Alarm List** button and click **Refresh**.

If the `Improper APS Codes` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-48: Clear "inc. data type mismatch" alarm

Overview

This procedure is used to clear an `inc. data type mismatch` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. data type mismatch` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `inc. data type mismatch` alarm in the resulting alarm list.

2 Determine the alarm level(s) for the active `inc. data type mismatch` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, determine the affected VCG, and note the corresponding AID and the type of circuit pack.

Note: An LNW73/73C VCG must be connected through the network to another Fiber Channel VCG.

An Ethernet LNW63, LNW66, LNW67, LNW68 VCG must be connected through the network to another Ethernet VCG.

4 Using circuit layouts and/or office records, identify the far-end network element for the specified VCG.

5 Use the *WaveStar®* CIT to log in to the required far-end Alcatel-Lucent 1665 DMX for the specified VCG.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

6 From the System View, select **Reports** → **Equipment Lists** → **Pack**. Select *Shelf* and click **Select**.

Result: The *Circuit Pack List* appears.

7 Using the *Circuit Pack List* and office records, determine if the far-end pack is the same type (Ethernet, Fibre Channel) as the near end circuit pack.

8

If the far-end Alcatel-Lucent 1665 DMX...	Then...
Is the same type of circuit pack as the near end,	Proceed to Step 11.
Is a different type of circuit pack than the near end,	Decide which circuit pack should be replaced so the types match. Change one of the circuit packs to match the other end. Continue with the next step.

9 From the System View, click the **Alarm List** button and click **Refresh**.

10 Is the `inc. data type mismatch` alarm still present?

If...	Then...
Yes	Continue the next step.
No	STOP! End of Procedure.

11 At the near end, select **View** → **Cross-Connections**. Select the required circuit pack and click **Select** to obtain a list of cross-connections. Observe the provisioned cross-connections for the required circuit pack and verify that the port is connected through the network to a circuit pack of the same type.

Note: The cross-connections at the local node may be correct; the incorrect cross-connection could be at any node in the transmission path.

12 Select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and make the required cross-connections changes to/from the circuit pack.

13 From the System View, click the **Alarm List** button and click **Refresh**.

14 Is the `inc. data type mismatch` alarm still present?

If...	Then...
Yes	Continue the next step.
No	STOP! End of Procedure.

15 From the System View, select **View** → **Equipment**, expand the group (GRP), highlight the alarmed port, and then click **Select**.

Result: The *View Equipment* window opens.

16

If the affected port is...	Then...
Connected to test equipment,	Proceed to Step 17.
In service,	Proceed to Step 18.

17 If the port is connected to test equipment, you have the following options to clear the alarm.

1. Align the test set signal characteristics with those of the port.
2. Disconnect the test set, or
3. Ignore the alarm until the test set is disconnected, (*recommended method*), or

18 In the Transmission section of the *Configure Equipment* window, change the provisioned state of the VCG's GFP Frame Check Sequence (ENABLE or DISABLE) to match the far end port and click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes**. Continue with Step 19.

19 Click **Close** on the *Configure Equipment* window.

20 From the System View, click the **Alarm List** button and click **Refresh**.

21 Is the `inc. data type mismatch` alarm still present?

If...	Then...
Yes	Contact your next level of support.
No	STOP! End of Procedure.

END OF STEPS

Procedure 5-49: Clear "inc. DS1/E1 sync. ref." alarms

Overview

This procedure is used to clear the following alarms:

- `inc. DS1 sync. ref. AIS`
- `inc. DS1 sync. ref. BER`
- `inc. DS1 sync. ref. EOOF`
- `inc. DS1 sync. ref. LOF`
- `inc. DS1 sync. ref. LOS`
- `inc. DS1 sync. ref. OOL`
- `inc. E1 sync. ref. AIS`
- `inc. E1 sync. ref. BER`
- `inc. E1 sync. ref. CRC-4 MFA mismatch`
- `inc. E1 sync. ref. LOF`
- `inc. E1 sync. ref. LOS`
- `inc. E1 sync. ref. OOL`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Select **View** → **Equipment** to determine if the Main slots are equipped with Very Large Fabric circuit packs.

Steps

Complete the following steps to clear an `inc. DS1/E1 sync. ref` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. DS1/E1 sync. ref` alarm in the resulting alarm list and note the corresponding AID.

2 Is the alarm `inc. DS1 sync. ref. EOOF`?

If...	Then...
Yes	No action necessary, alarm automatically clears at midnight.
No	Continue with the next step.

3 Is the alarm `inc. DS1/E1 sync. ref. OOL`?

If...	Then...
Yes and the Main slots are *not* equipped with Very Large Fabric (VLF) circuit packs	Perform the following: 1. Repair the Timing references according to local procedures. 2. From the System View, select **Configuration** → **Update System** → **Update Reference**. **Result:** A dialog box appears asking you to confirm executing this command. Click **Yes.** STOP! End of Procedure.
Yes and the Main slots are equipped with Very Large Fabric (VLF) circuit packs	Proceed to Step 6.
No	Continue with the next step.

4 Is the alarm `inc. E1 sync. ref. CRC-4 MFA mismatch`?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 6.

5 To clear the `inc. E1 sync. ref. CRC-4 MFA mismatch` alarm, either change the format of the incoming E1 synchronization reference signal to CRC-4 or change the format of the local E1 timing input port to FAS (Frame Alignment Signal) according to local procedures.

If changing the format of the...	Then...
incoming E1 synchronization reference signal,	notify personnel at the site supplying the E1 synchronization reference signal to change the format to CRC-4.
local E1 timing input port,	Use **Configuration** → **Timing/Sync** to access the Timing Input port and provision the *Input and Output Format* parameter to FAS. **Result:** Click **OK**. A warning message may appear. Click **Yes** to execute the command.

STOP! End of Procedure.

6 **Important!** Perform the following to clear `inc. sync. ref. AIS`, `inc. DS1/E1 sync. ref. BER`, `inc. DS1/E1 sync. ref. LOF`, and `inc. DS1/E1 sync. ref. LOS` alarms. This also includes `inc. DS1/E1 sync. ref. OOL` alarms (VLF mains only).

Visually check the incoming signal cables and connections and correct any problems found. If a visual inspection does not reveal any problems, you may consider making electrical measurements per local procedures.

7 From the System View, click the **Alarm List** button and click **Refresh**.

8 Is the `inc. DS1/E1 sync. ref` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

9 Follow local procedures to isolate and repair the trouble.

END OF STEPS

Procedure 5-50: Clear "inc. (from DSX) DS1" alarms

Overview

This procedure is used to clear the following `inc. DS1` alarms:

- `inc. (from DSX) DS1 AIS`
- `inc. (from DSX) DS1 LOF`
- `inc. (from DSX) DS1 LOS`
- `inc. (from DSX) DS1 sig. failed`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. DS1` alarm.

---

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. DS1` alarm in the resulting alarm list.

---

2 Determine the alarm level(s) for the active `inc. DS1` alarm(s). Clear the alarms in order of severity.

---

3 Refer to the Probable Cause column in the alarm list, determine the affected port, and note the corresponding AID.

---

4 Check cable connections between the access panel and the DSX panel for faulty connections or damage and repair/replace as necessary.

---

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. DS1` alarm still present?

If...	Then...
Yes	Continue with Step 7.
No	STOP! End of Procedure.

7 Is the alarm an `inc. DS1 LOF`?

If...	Then...
Yes	Determine and record the signal format and the line code of the interfacing customer port connected to the alarmed port on the local network element and then continue with Step 8
No	Proceed to Step 12.

8 From the Alcatel-Lucent 1665 DMX System View, select **View** → **Equipment**, expand the pack, expand the VT group, highlight the alarmed port and click **Select**.

9 Compare the signal format and the line code of the local DS1 port against the information determined about the interfacing customer port. If there are inconsistencies, determine the correct provisioning and correct according to local procedures.

If the local DS1 port is provisioned incorrectly, from the System View, select **Configuration** → **Equipment**, expand the pack, expand the VT group, highlight the alarmed port and click **Select**. Provision the Signal Format and the Line Code appropriately, click **Apply**, and then click **Close**.

10 From the System View, click the **Alarm List** button and click **Refresh**.

11 Is the `inc. DS1` alarm still present?

If...	Then...
Yes	Continue with Step 12.
No	STOP! End of Procedure.

12 **Important!** A likely cause of an `inc. DS1` alarm at the local network element is a failure at the interfacing customer DS1 port or a problem with the cabling/wiring between systems.

Follow local procedures to isolate and clear the trouble.

END OF STEPS

Procedure 5-51: Clear "inc. (from DSX) DS3" alarms

Overview

This procedure is used to clear the following `inc. DS3` alarms:

- `inc. (from DSX) DS3 AIS`
- `inc. (from DSX) DS3 IDLE`
- `inc. (from DSX) DS3 LOF`
- `inc. (from DSX) DS3 LOS`
- `inc. (from DSX) DS3 sig. failed`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. DS3` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `inc. DS3` alarm in the resulting alarm list.

2 Determine the alarm level(s) for the active `inc. DS3` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, determine the affected port, and note the corresponding AID.

4 Check cable connections between the backplane and the DSX panel for faulty connections or damage and repair/replace as necessary.

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. DS3` alarm still present?

If...	Then...
Yes	Continue with Step 7.
No	STOP! End of Procedure.

7 Is the alarm an `inc. DS3 LOF`?

If...	Then...
Yes	Determine and record the signal format of the interfacing customer port connected to the alarmed port on the local network element and then continue with Step 8.
No	Proceed to Step 12.

8 From the Alcatel-Lucent 1665 DMX System View, select **View** → **Equipment**, expand the pack, highlight the alarmed port, and click **Select**.

9 Compare the signal format of the local port against the information determined about the interfacing customer port. If there are inconsistencies, determine the correct provisioning and correct according to local procedures.

If the local port is provisioned incorrectly, from the System View, select **Configuration** → **Equipment**, expand the pack, highlight the alarmed port, and click **Select**. Provision the Signal Format appropriately, click **Apply**, and then click **Close**.

10 From the System View, click the **Alarm List** button and click **Refresh**.

11 Is the `inc. DS3` alarm still present?

If...	Then...
Yes	Continue with Step 12.
No	STOP! End of Procedure.

12 **Important!** A likely cause of an `inc. DS3` alarm at the local network element is a failure at the interfacing customer DS3 port or a problem with the cabling/wiring between systems.

Follow local procedures to isolate and clear the trouble.

END OF STEPS

Procedure 5-52: Clear "inc. DS3 Cbit Mismatch" alarm

Overview

This procedure is used to clear an `inc. DS3 Cbit Mismatch` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear an `inc. DS3 Cbit Mismatch` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. DS3 Cbit Mismatch` alarm in the resulting alarm list and note the corresponding AID.

2 From the System View, select **View** → **Equipment**, expand the group (GRP), highlight the alarmed port, and then click **Select**.

Result: The *View Equipment* window opens.

3 In the Transmission section on the window, locate and record the provisioned signal format.

4 From the System View, select **Configuration** → **Equipment**, expand the group (GRP), highlight the desired port, and then click **Select**.

Result: The *Configure Equipment* window opens.

5

If the affected port is...	Then...
Looped back on itself using patch cords at the local DSX-3 panel or equivalent connection point,	Continue with Step 6.
Connected to test equipment,	Proceed to Step 8.

If the affected port is...	Then...
In service,	Proceed to Step 10.

6 If the port is provisioned as Framed (M13) format, and it is looped back on itself using patch cords at the local DSX-3 panel or equivalent connection point, you have the following options to clear the alarm.

1. Remove the patch cords at the local DSX-3 panel or equivalent connection point, or
2. Ignore the alarm until the loopback is removed, (*recommended method*), or
3. Change the provisioning of the port that is looped back (continue with Step 7.) *This method is not recommended.* The port must be reprovisioned after the loopback is removed.

7 In the Transmission section of the *Configure Equipment* window, change the Signal Format parameter for the port to either C-Bit or Clear Channel and click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes**. Proceed to Step 11.

8 If the port is connected to test equipment, you have the following options to clear the alarm.

1. Change the test set DS3 set-up to match the Signal Format parameter for that port: either Framed (M13), C-bit, or Clear Channel, or
2. Disconnect the test set, or
3. Ignore the alarm until the test set is disconnected, (*recommended method*), or
4. Change the provisioning of the port that is connected to the test equipment (continue with Step 9). *This method is not recommended.* The port must be reprovisioned after the test set is disconnected.

9 In the Transmission section of the *Configure Equipment* window, change the Signal Format parameter for that port to match the test set DS3 set-up: either Framed (M13), C-Bit, or Clear Channel and click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes**. Proceed to Step 11.

10 In the Transmission section of the *Configure Equipment* window, change the Signal Format parameter for that port to Clear Channel or another appropriate signal type and click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes**. Continue with Step 11.

11 Click **Close** on the *Configure Equipment* window.

END OF STEPS

Procedure 5-53: Clear "inc. (from DSX) DSn RAI" alarm

Overview

This procedure is used to clear the following:

- `inc. (from DSX) DS1 RAI`
- `inc. (from DSX) DS3 RAI`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Task

Complete the following steps to clear an `inc. (from DSX) DSn RAI` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. (from DSX) DSn RAI` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected DSn port, and note the corresponding AID.

3 **Important!** The `inc. (from DSX) DSn RAI` alarm indicates that the interfacing customer equipment that terminates the DSn signal has detected a bad DSn signal from this network element.

Check cable connections between the access panel and the DSX panel or equivalent connection point for faulty connections or damage and repair/replace as necessary.

4 From the System View, click the **Alarm List** button and click **Refresh**.

5 Is the `inc. (from DSX) DSn RAI` alarm still present?

If...	Then...
Yes	Continue with Step 6.
No	STOP! End of Procedure.

6 **Important!** At this point, the local network element is operating correctly. The trouble is in the interfacing customer equipment that terminates the DSn signal or in the cabling between the DSn port and the interfacing customer equipment.

Follow local procedures for addressing DSn-related conditions/alarms at the interfacing customer equipment that terminates the DSn signal.

7 From the System View at the local network element, click the **Alarm List** button and click **Refresh**.

8 Is the `inc. (from DSX) DSn RAI` condition/alarm still present?

If...	Then...
Yes	Continue with Step 9.
No	STOP! End of Procedure.

9 Follow local procedures to isolate and clear the cable trouble between interfacing customer equipment that terminates the DSn signal and the DSn port.

END OF STEPS

Procedure 5-54: Clear "inc. (from fiber) DSn" alarms

Overview

This procedure is used to clear the following alarms:

- `inc. (from fiber) DS1 AIS`
- `inc. (from fiber) DS1 LOF`
- `inc. (from fiber) DS3 AIS`
- `inc. (from fiber) DS3 LOF`

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.
3. Obtain office records showing the correct port provisioning values for the affected local port.

Steps

Complete the following steps to clear an `inc. (from fiber) DSn` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. (from fiber) DSn` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected port, and note the corresponding AID.

3 Select **View** → **Equipment** to access the affected port and click **Select**.

Result: The port parameters appear.

4 Compare the provisioned port parameter values with office records.

If the local port is provisioned incorrectly, select **Configuration** → **Equipment** to access the affected port and click **Select**. Provision the port parameters as required and click **Apply**. Then click **Close**.

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. (from fiber) DSn` alarm still present?

If...	Then...
Yes	Continue the next step.
No	STOP! End of Procedure.

7 Using circuit layouts and/or office records, identify the other network element where the alarmed DSn is terminated.

8 **Important!** A likely cause of an `inc. (from fiber) DSn` alarm at the local network element is a problem/failure at either the far-end SONET network element or the interfacing customer equipment connected to the far-end SONET network element.

Follow local procedures for addressing any DSn-related alarms/conditions at the far-end SONET network element or the interfacing customer equipment connected to the far-end SONET network element.

END OF STEPS

Procedure 5-55: Clear "inc. (from fiber) DSn RAI" alarms

Overview

This procedure is used to clear the following alarms:

- `inc. (from fiber) DS1 RAI`
- `inc. (from fiber) DS3 RAI`

Before you begin

Prior to performing this task:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Task

Complete the following steps to clear an `inc. (from fiber) DSn RAI` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. (from fiber) DSn RAI` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected port, and note the corresponding AID.

3 Using circuit layouts and/or office records, identify the other network element where the alarmed DSn is terminated.

4 **Important!** A likely cause of the `inc. (from fiber) DSn RAI` alarm at the local network element is a problem/failure at the interfacing customer equipment that is connected to the far-end SONET network element.

Follow local procedures for addressing any DSn-related conditions/alarms at the interfacing customer equipment that is connected to the far-end SONET network element.

END OF STEPS

Procedure 5-56: Clear "inc. (from DSX) E1" alarms

Overview

This procedure is used to clear the following `inc. E1` alarms:

- `inc. (from DSX) E1 AIS`
- `inc. (from DSX) E1 LOF`
- `inc. (from DSX) E1 LOS`
- `inc. (from DSX) E1 sig. failed`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. E1` alarm.

---

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. E1` alarm in the resulting alarm list.

---

2 Determine the alarm level(s) for the active `inc. E1` alarm(s). Clear the alarms in order of severity.

---

3 Refer to the Probable Cause column in the alarm list, determine the affected port, and note the corresponding AID.

---

4 Check cable connections between the access panel and the DSX panel for faulty connections or damage and repair/replace as necessary.

---

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. E1` alarm still present?

If...	Then...
Yes	Continue with Step 7.
No	STOP! End of Procedure.

7 Is the alarm an `inc. E1 LOF`?

If...	Then...
Yes	Determine and record the signal format and the line code of the interfacing customer port connected to the alarmed port on the local network element and then continue with Step 8.
No	Proceed to Step 12.

8 From the Alcatel-Lucent 1665 DMX System View, select **View** → **Equipment**, expand the circuit pack and TUG signals, highlight the alarmed port and click **Select**.

9 Compare the signal format and the line code of the local port against the information determined about the interfacing customer port. If there are inconsistencies, determine the correct provisioning and correct according to local procedures.

If the local port is provisioned incorrectly, from the System View, select **Configuration** → **Equipment**, expand the pack and TUG signals, highlight the alarmed port and click **Select**. Provision the Signal Format appropriately, click **Apply**, and then click **Close**.

10 From the System View, click the **Alarm List** button and click **Refresh**.

11 Is the `inc. E1` alarm still present?

If...	Then...
Yes	Continue with Step 12.
No	STOP! End of Procedure.

12 **Important!** A likely cause of an `inc. E1` alarm at the local network element is a failure at the interfacing customer E1 port or a problem with the cabling/wiring between systems.

Follow local procedures to isolate and clear the trouble.

END OF STEPS

Procedure 5-57: Clear "inc. EC1" alarms

Overview

This procedure is used to clear all `inc. EC1` alarms, including:

- `inc. EC1 line AIS`
- `inc. EC1 LOF`
- `inc. EC1 LOS`
- `inc. EC1 RFI-L`
- `inc. EC1 sig. degrade (BER)`
- `inc. EC1 sig. failed (BER)`
- `inc. STS LOP`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. EC1` alarm.

---

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. EC1` alarm in the resulting alarm list.

---

2 Determine the alarm level(s) for the active `inc. EC1` alarm(s). Clear the alarms in order of severity.

---

3 Refer to the Probable Cause column in the alarm list, determine the affected port, and note the corresponding AID.

---

4 Check cable connections between the shelf and the cross-connect panel (or equivalent) for faulty connections/damage and repair/replace as necessary.

---

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. EC1` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

7 **Important!** A likely cause of an `inc. EC1` alarm at the local network element is a failure at the interfacing customer EC1 port or a problem with the cabling/wiring between systems.

Follow local procedures to isolate and clear the trouble.

END OF STEPS

Procedure 5-58: Clear "inc. FE-LAN ANM" alarm

Overview

This procedure is used to clear an `inc. FE-LAN ANM` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. FE-LAN ANM` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. FE-LAN ANM` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding AID.

3 From the System View, select **View** → **Equipment**, expand the required circuit pack, highlight the alarmed port, and click **Select**. Then click the *Port Data* tab.

Result: The port parameters appear. The port parameters vary according to the circuit pack.

4 Record the following information:

- Provisioned Duplex Mode (LNW66 only)
- Actual Duplex Mode Operation (LNW66 only)
- Provisioned Line Rate (electrical Fast Ethernet ports only)
- Actual Line Rate Operation (electrical Fast Ethernet ports only)

5 From the *View Equipment* window, click *Flow Control* tab.

Result: The flow control parameters appear.

6 Record the following information:

- Provisioned Flow Control Mode
- Flow Control Mode Operation

Click **Close**.

7 Follow local procedures and determine the provisioned and actual (operational) duplex mode, line rate, and flow control mode at the interfacing customer LAN port.

8 Does the actual (operational) duplex mode, line rate, and flow control mode match on both the local LAN port and the interfacing customer LAN port?

If...	Then...
Yes	Proceed to Step 16.
No	Continue with Step 9.

9 Follow local procedures to determine if provisioning changes are required at the local LAN port or the interfacing customer LAN port.

If provisioning changes are required at the...	Then...
local LAN port,	Continue with Step 10.
interfacing customer LAN port,	Follow local procedures to resolve the provisioning conflicts then proceed to Step 16.

10 Do the actual (operational) duplex mode and line rate match on both the local LAN port and the interfacing customer LAN port?

If...	Then...
Yes	Proceed to Step 13.
No	Continue with Step 11.

11 From the System View select **Configuration** → **Equipment**, expand the required circuit pack, highlight the desired port, and click **Select**. Then click the *Port Data* tab.

Result: The port parameters appear.

12 Provision the *Provisioned Duplex Mode* and/or *Line Rate* parameters as required to match the interfacing customer LAN port and click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes**.

13 Does the actual (operational) flow control modes match on both the local LAN port and the interfacing customer LAN port?

If...	Then...
Yes	Proceed to Step 16.
No	Continue with Step 14.

14 From the System View, select **Configuration** → **Equipment**, expand the required circuit pack, highlight the desired port and click **Select**. Then click the *Flow Control* tab.

Result: The flow control parameters appear.

15 Provision the *Flow Control Mode* parameter as required to match the interfacing customer LAN port and click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes**.

16 From the System View, click the **Alarm List** button and click **Refresh**.

17 Is the `inc. FE-LAN ANM` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

18 From the System View select **Configuration** → **Equipment**, expand the required circuit pack, highlight the desired port, and click **Select**. Then click the *Port Data* tab.

Result: The port parameters appear.

19 **Disable** the *Auto-Negotiation* parameter and click **Apply**. Then **Enable** the *Auto-Negotiation* parameter and click **Apply**.

20 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inc. FE-LAN ANM` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-59: Clear "inc. FE-LAN FEFI" alarm

Overview

This procedure is used to clear an `inc. FE-LAN FEFI` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. FE-LAN FEFI` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. FE-LAN FEFI` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding Fast Ethernet LAN port AID.

3 **Important!** The `inc. FE-LAN FEFI` alarm indicates that the interfacing customer equipment has detected a bad incoming Fast Ethernet signal from this network element. The `inc. FE-LAN FEFI` alarm is normally cleared by addressing other alarms/conditions.

Are there other alarms/conditions in the alarm list?

If...	Then...
Yes	Proceed to the appropriate procedures to clear the alarms in order of severity. Then continue with the next step.
No	Proceed to Step 6.

4 From the System View, click the **Alarm List** button and click **Refresh**.

5 Is the `inc. FE-LAN FEFI` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

6 Visually check the local transmit cable connections between the shelf and the patch panel or equivalent connection point for faulty connections or damage.

If faulty connections or damage...	Then...
was found,	Follow local procedures to repair/replace as necessary. Then continue with the next step.
was *not* found,	Proceed to Step 9.

7 From the System View, click the **Alarm List** button and click **Refresh**.

8 Is the `inc. FE-LAN FEFI` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

9

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local Ethernet circuit pack.

Reference: Procedure 6-7: "Replace Ethernet/Data circuit pack" (p. 6-68)

10 From the System View, click the **Alarm List** button and click **Refresh**.

11 Is the `inc. FE-LAN FEFI` alarm still present?

If...	Then...
Yes	Remove the replacement circuit pack and return the original circuit pack to the slot, then continue with the next step.
No	STOP! End of Procedure.

12 **Important!** At this point, the local network element is operating correctly. The trouble is in the interfacing customer equipment or in the cable between the interfacing customer equipment and the local network element.

Follow local procedures for addressing conditions/alarms at the interfacing customer equipment.

13 From the System View at the local network element, click the **Alarm List** button and click **Refresh**.

14 Is the `inc. FE-LAN FEFI` condition/alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

15 Follow local procedures to isolate and clear the cable trouble between the interfacing customer equipment and the local network element.

16 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inc. FE-LAN FEFI` alarm is still present, contact you next level of support.

END OF STEPS

Procedure 5-60: Clear "inc. FE-LAN LOS" alarm

Overview

This procedure is used to clear an `inc. FE-LAN LOS` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. FE-LAN LOS` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. FE-LAN LOS` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding AID.

3 Using office records, determine if the LAN port is supposed to be in service.

If the LAN port is...	Then...
supposed to be in service,	Continue with Step 4.
not supposed to be in service,	From the System View, select **Configuration** → **Update System** → **Update States**. Then proceed to Step 8

4 Check local cable connections between the shelf backplane/faceplate and the interconnecting equipment for faulty connections or damage and repair/replace as necessary.

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. FE-LAN LOS` alarm still present?

If...	Then...
Yes	Continue with Step 7.
No	STOP! End of Procedure.

7 **Important!** A likely cause of the alarm is a failure at the interfacing customer LAN equipment or a problem with cabling/wiring between the local LAN port and the interfacing customer LAN equipment.

Follow local procedures to isolate and clear the trouble.

8 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inc. FE-LAN LOS` alarm is still present, contact you next level of support.

END OF STEPS

Procedure 5-61: Clear "inc. GE-LAN ANM" alarm

Overview

This procedure is used to clear an `inc. GE-LAN ANM` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to"Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. GE-LAN ANM` alarm.

---

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `inc. GE-LAN ANM` alarm in the resulting alarm list.

---

2 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding AID.

---

3 From the System View, select **View** → **Equipment**, expand the required circuit pack, highlight the alarmed port, and click **Select**. Then click the *Flow Control* tab.

Result: The flow control parameters appear.

---

4 Record the following information:

- Provisioned Flow Control Mode
- Flow Control Mode Operation

Click **Close**.

---

5 Follow local procedures and determine the provisioned and actual (operational) flow control mode at the interfacing customer LAN port.

6 Does the actual (operational) flow control mode match on both the local LAN port and the interfacing customer LAN port?

If...	Then...
Yes	Proceed to Step 10.
No	Continue with Step 7.

7 Follow local procedures to determine if provisioning changes are required at the local LAN port or the interfacing customer LAN port.

If provisioning changes are required at the...	Then...
local LAN port,	Continue with Step 8.
interfacing customer LAN port,	Follow local procedures to resolve the provisioning conflicts then proceed to Step 10.

8 From the System View, select **Configuration** → **Equipment**, expand the required circuit pack, highlight the desired port and click **Select**. Then click the *Flow Control* tab.

Result: The flow control parameters appear.

9 Provision the *Flow Control Mode* parameter as required to match the interfacing customer LAN port and click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes**.

10 From the System View, click the **Alarm List** button and click **Refresh**.

11 Is the `inc. GE-LAN ANM` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

12 From the System View select **Configuration** → **Equipment**, expand the required circuit pack, highlight the desired port, and click **Select**. Then click the *Port Data* tab.

Result: The port parameters appear.

13 **Disable** the *Auto-Negotiation* parameter and click **Apply**. Then **Enable** the *Auto-Negotiation* parameter and click **Apply**.

14 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inc. GE-LAN ANM` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-62: Clear "inc. GE-LAN LOS" alarm

Overview

This procedure is used to clear an `inc. GE-LAN LOS` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. GE-LAN LOS` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. GE-LAN LOS` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding AID.

3 Using office records, determine if the LAN port is supposed to be in service.

If the LAN port is...	Then...
supposed to be in service,	Continue with Step 4.
not supposed to be in service,	From the System View, select **Configuration** → **Update System** → **Update States**. Then proceed to Step 8

4 Check local fiber/cable connections between the LAN port and the interconnecting equipment for faulty connections or damage and clean/repair/replace as necessary.

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. GE-LAN LOS` alarm still present?

If...	Then...
Yes	Continue with Step 7.
No	STOP! End of Procedure.

7 **Important!** A likely cause of the alarm is a failure at the interfacing customer LAN equipment or a problem with fiber/cable between the local LAN port and the interfacing customer LAN equipment.

Follow local procedures to isolate and clear the trouble.

8 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inc. GE-LAN LOS` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-63: Clear "inc. line sync. ref. OOL" alarm

Overview

This procedure is used to clear the `inc. line sync. ref. OOL` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Select **View** → **Equipment** to determine if the Main slots are equipped with Very Large Fabric circuit packs.

Steps

Complete the following steps to clear `inc. line sync. ref. OOL` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button, locate the `inc. line sync. ref. OOL` alarm in the resulting alarm list.

2 Refer to the Probable Cause column (SYNCOOS or SYNC) in the alarm list, determine the affected OC-N line, and note the corresponding AID.

3 Are there any `inc. OCN` alarms present in the alarm list?

If...	Then...
Yes,	Proceed to the appropriate procedure to clear each alarm in order of severity. Then continue with the next step.
No,	Proceed to Step 7.

4 If the Main slots are equipped with non-VLF circuit packs, select **Configuration** → **Update System** → **Update Reference**.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes.**

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. line sync. ref. OOL` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

7 **Important!** A possible cause of the alarm at the local node is a synchronization problem at the far-end (upstream) node that causes the TX interfaces (at the far-end node) to transmit off frequency.

Using office records, identify and log in to the far-end SONET network element supplying the optical signal.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

8 Follow local procedures for addressing synchronization- and OCN-related conditions/alarms at the far-end SONET network element.

9 If the Main slots are equipped with non-VLF circuit packs at the local node, select **Configuration** → **Update System** → **Update Reference**.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes.**

10 From the System View at the local node, click the **Alarm List** button and click **Refresh**.

11 Is the `inc. line sync. ref. OOL` alarm still present?

If...	Then...
Yes	Continue with the next step.

If...	Then...
No	STOP! End of Procedure.

12 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local OC-N OLIU circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

13 If the Main slots are equipped with non-VLF circuit packs, select **Configuration** → **Update System** → **Update Reference**.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes.**

14 From the System View, click the **Alarm List** button and click **Refresh**.

15 Is the `inc. line sync. ref. OOL` alarm still present?

If...	Then...
Yes	Remove the replacement OC-N OLIU circuit pack and return the original circuit pack to the slot, then contact your next level of support.
No	STOP! End of Procedure.

END OF STEPS

Procedure 5-64: Clear "inc. LAG" alarms

Overview

This procedure is used to clear the following alarms:

- `inc. LAG Partial Link Loss`
- `inc. LAG PLCF`
- `inc. LAG Total Link Loss`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. LAG` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. LAG` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected Link Aggregation Group, and note the corresponding AID.

3 **Important!** A likely cause of the `inc. LAG` alarm is a transmission-related LAN port or socket alarm/standing condition associated with a member of the Link Aggregation Group.

Refer to the alarm list and note all LAN port and socket alarms/standing conditions associated with members of the specified Link Aggregation Group.

4 Proceed to the appropriate procedures to clear all LAN port and socket alarms/standing conditions associated with members of the specified Link Aggregation Group in order of severity.

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. LAG` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

7 Visually check the local fiber connections between the affected circuit pack faceplate/pluggable transmission modules and the LGX panel or equivalent connection point to ensure that the LAN ports are properly connected.

If improper connections...	Then...
were found,	Follow local procedures to connect the LAN ports as required. Then continue with Step 8.
were *not* found,	Proceed to Step 10.

8 From the System View, click the **Alarm List** button and click **Refresh**.

9 Is the `inc. LAG` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

10 **Important!** A likely cause of the `inc. LAG` alarm at the local network element is a configuration conflict with the interfacing customer LAN port (LAG partner). The Link Aggregation Group and/or LAN port provisioning at the LAG partner is incompatible.

Follow local procedures to verify the Link Aggregation Group and/or LAN port provisioning at the interfacing customer LAN port (LAG partner). Does the LAG partner have Link Aggregation Control Protocol (LACP) enabled?

If...	Then...
Yes,	Proceed to Step 13.

If...	Then...
No,	At the local node, select **Configuration** → **Data** → **Create/Modify/Delete LA Group** to access the required local Link Aggregation Group and provision the *Protocol* parameter to **None** to disable the Link Aggregation Control Protocol. Continue with the next step.

11 From the System View, click the **Alarm List** button and click **Refresh**.

12 Is the `inc. LAG` alarm still present?

If...	Then...
Yes	Contact your next level of support.
No	STOP! End of Procedure.

13 At the local node, select **View** → **Data** → **Virtual Switch** to access the Virtual Switch associated with the required local Link Aggregation Group and determine the provisioned *VLAN Tagging Mode* (802.1TAG or Transparent).

14

If the provisioned VLAN Tagging Mode is...	Then...
802.1TAG,	Select **View** → **Data** → **VLAN** to access the assigned VLANs and verify that a VLAN is provisioned for the required Link Aggregation Group listed under *Ethernet Port (Untagged)*. If required, select **Configuration** → **Data** → **Create VLAN** to provision a VLAN for Untagged Traffic on the required Link Aggregation Group.

If the provisioned VLAN Tagging Mode is...	Then...
Transparent,	Select **View** → **Data** → **Port Tag** to access the assigned Port Tags and verify that a Port Tag is provisioned for the required Link Aggregation Group listed under *Ethernet Port (Default Tag)*. If required, select **Configuration** → **Data** → **Create Port Tag** to provision a Default Tag for the required Link Aggregation Group.

15 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inc. LAG` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-65: Clear "inc. LOS" alarm

Overview

This procedure is used to clear an `inc. LOS` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. LOS` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. LOS` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack affected, and note the corresponding AID.

3 Using office records, determine if the Data port is supposed to be in service.

If the Data port is...	Then...
supposed to be in service,	Continue with Step 4.
not supposed to be in service,	From the System View, select **Configuration** → **Update System** → **Update States**. Then proceed to Step 8.

4 Check local fiber/cable connections between the Data port and the interconnecting equipment for faulty connections or damage and clean/repair/replace as necessary.

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. LOS` alarm still present?

If...	**Then...**
Yes	Continue with Step 7.
No	STOP! End of Procedure.

7 **Important!** A likely cause of the alarm is a failure at the interfacing customer Data equipment or a problem with fiber/cable between the local Data port and the interfacing customer Data equipment.

Follow local procedures to isolate and clear the trouble.

8 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inc. LOS` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-66: Clear "inc. Loss of Synch" alarm

Overview

This procedure is used to clear an `inc. Loss of Synch` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. Loss of Synch` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. Loss of Synch` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding port AID.

3 Check local fiber/cable connections between the affected port and the interconnecting equipment for faulty connections or damage and clean/repair/replace as necessary.

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

4 From the System View, click the **Alarm List** button and click **Refresh**.

5 Is the `inc. Loss of Synch` alarm still present?

If...	Then...
Yes	Continue with Step 6.
No	STOP! End of Procedure.

6 **Important!** A likely cause of the alarm is a failure at the interfacing customer equipment or a problem with fiber/cable between the affected port and the interfacing customer equipment.

Follow local procedures to isolate and clear the trouble.

7 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inc. Loss of Synch` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-67: Clear "inc. MUX OCH LOS-P" alarm

Overview

This procedure is used to clear an `inc. MUX OCH LOS-P` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. MUX OCH LOS-P` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. MUX OCH LOS-P` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding OCH port AID.

3 Using office records, determine if the OCH port is supposed to be in service.

If the OCH port is...	Then...
supposed to be in service,	Continue with the next step.
not supposed to be in service,	From the System View, select **Configuration** → **Update System** → **Update States**. STOP! End of Procedure.

4 Check local fiber/cable connections between the affected OCH port and the transmitting optical circuit pack/port for faulty connections or damage and clean/repair/replace as necessary.

Reference: Procedure 6-11: “Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)” (p. 6-151)

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. MUX OCH LOS-P` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

7 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected OMD circuit pack.

Reference: Procedure 6-28: “Replace DWDM optical multiplexer/demultiplexer circuit pack” (p. 6-294)

8 From the System View, click the **Alarm List** button and click **Refresh**.

9 Is the `inc. MUX OCH LOS-P` alarm still present?

If...	Then...
Yes	Remove the replacement circuit pack and return the original circuit pack to the slot, then continue with the next step.
No	STOP! End of Procedure.

10 Is the transmitting OLIU circuit pack equipped with pluggable transmission modules?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 14.

11 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected transmitting pluggable transmission module.

Reference: Procedure 6-8: “Replace pluggable transmission module” (p. 6-71)

12 From the System View, click the **Alarm List** button and click **Refresh**.

13 Is the `inc. MUX OCH LOS-P` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

14 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected transmitting OLIU circuit pack.

Reference: Procedure 6-5: “Replace high-speed main OLIU circuit pack” (p. 6-48)

15 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inc. MUX OCH LOS-P` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-68: Clear "inc. OCN" alarms

Overview

This procedure is used to clear the following `inc. OCN` alarms:

- `inc. OCN line AIS`
- `inc. OCN LOF`
- `inc. OCN LOS`
- `inc. OCN sig. degrade (BER)`
- `inc. OCN sig. failed (BER)`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear `inc. OCN` alarms.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. OCN` alarm in the resulting alarm list.

2 Determine the alarm level(s) for the active `inc. OCN` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, determine the affected OC-N line, and note the corresponding AID.

4 Visually check the local receive fiber connections between the circuit pack faceplate/pluggable transmission module and the LGX panel or equivalent connection point for faulty connections or damage.

If faulty connections or damage...	Then...
was found,	Follow local procedures to repair/replace as necessary. Then continue with Step 5.
was *not* found,	Proceed to Step 7.

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. OCN` alarm still present?

If...	Then...
Yes	Continue with Step 7.
No	STOP! End of Procedure.

7

If the affected OC-N OLIU circuit pack is...	Then...
equipped with pluggable transmission modules,	Continue with Step 8.
not equipped with pluggable transmission modules,	Proceed to Step 11.

8 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a luggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local pluggable transmission module.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

9 From the System View, click the **Alarm List** button and click **Refresh**.

10 Is the `inc. OCN` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with Step 11.
No	STOP! End of Procedure.

11

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local OC-N OLIU circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

12 From the System View, click the **Alarm List** button and click **Refresh**.

13 Is the `inc. OCN` alarm still present?

If...	Then...
Yes	Remove the replacement OC-N OLIU circuit pack and return the original circuit pack to the slot, then continue with Step 14.
No	STOP! End of Procedure.

14 **Important!** At this point, the local network element is operating correctly. The trouble is in the far-end network element or in the fiber/cable between the far-end network element and the local network element.

Follow local procedures for addressing OCN-related conditions/alarms at the far-end network element.

15 From the System View at the local network element, click the **Alarm List** button and click **Refresh**.

16 Is the `inc. OCN` alarm still present?

If...	Then...
Yes	Continue with Step 17.
No	STOP! End of Procedure.

17 Follow local procedures to isolate and clear the fiber/cable trouble between the far-end network element and the local network element.

END OF STEPS

Procedure 5-69: Clear "inc. OCN RFI-L" alarm

Overview

This procedure is used to clear an `inc. OCN RFI-L` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. OCN RFI-L` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. OCN RFI-L` alarm in the resulting alarm list.

2 **Important!** The `inc. OCN RFI-L` alarm indicates that the far-end network element has detected a bad OC-N signal from this network element. The `inc. OCN RFI-L` alarm is normally cleared by addressing other alarms/conditions.

Are there other conditions/alarms in the alarm list?

If...	Then...
Yes	Proceed to the appropriate procedures to clear the alarms in order of severity. Then continue with the next step.
No	Proceed to Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `inc. OCN RFI-L` alarm still present?

If...	Then...
Yes	Continue with the next step.

If...	Then...
No	STOP! End of Procedure.

5 Visually check the local transmit fiber connections between the circuit pack faceplate and the LGX panel or equivalent connection point for faulty connections or damage.

If faulty connections or damage...	Then...
was found,	Follow local procedures to repair/replace as necessary. Then continue with the next step.
was *not* found,	Proceed to Step 8.

6 From the System View, click the **Alarm List** button and click **Refresh**.

7 Is the `inc. OCN RFI-L` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

8 Is the OLIU circuit pack equipped with pluggable transmission modules?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 12.

9 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local pluggable transmission module.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

10 From the System View, click the **Alarm List** button and click **Refresh**.

11 Is the `inc. OCN RFI-L` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with Step 12.
No	STOP! End of Procedure.

12 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local OCn circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

13 From the System View, click the **Alarm List** button and click **Refresh**.

14 Is the `inc. OCN RFI-L` alarm still present?

If...	Then...
Yes	Remove the replacement OCn circuit pack and return the original circuit pack to the slot, then continue with Step 15.
No	STOP! End of Procedure.

15 **Important!** At this point, the local network element is operating correctly. The trouble is in the far-end network element or in the fiber/cable between the far-end network element and the local network element.

Follow local procedures for addressing OCN-related conditions/alarms at the far-end network element.

16 From the System View at the local network element, click the **Alarm List** button and click **Refresh**.

17 Is the `inc. OCN RFI-L` condition/alarm still present?

If...	Then...
Yes	Continue with Step 18.
No	STOP! End of Procedure.

18 Follow local procedures to isolate and clear the fiber/cable trouble between the far-end network element and the local network element.

END OF STEPS

Procedure 5-70: Clear "inc. ODU2 LCK/OCI" alarms

Overview

This procedure is used to clear the following `inc. ODU2/OTU2` alarms:

- `inc. ODU2 LCK`
- `inc. ODU2 OCI`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. ODU2 LCK/OCI` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. ODU2 LCK/OCI` alarm in the resulting alarm list and note the corresponding AID.

2 **Important!** The condition (trouble) is *not* in the local network element. There is a locked/open optical connection at an upstream network element.

Follow local procedures to isolate and clear the network trouble between the far-end network element and the local network element.

END OF STEPS

Procedure 5-71: Clear "inc. ODU2/OTU2" alarms

Overview

This procedure is used to clear the following `inc. ODU2/OTU2` alarms:

- `inc. ODU2 DEG`
- `inc. ODU2 SSF`
- `inc. OTU2 DEG`
- `inc. OTU2 LOF`
- `inc. OTU2 LOM`
- `inc. OTU2 LOS-P`
- `inc. OTU2 SSF`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear `inc. ODU2/OTU2` alarms.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. ODU2/OTU2` alarm in the resulting alarm list.

2 Determine the alarm level(s) for the active `inc. ODU2/OTU2` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, determine the affected OTU2/ODU2 port and note the corresponding AID.

4 Visually check the local receive fiber connections between the XM10G/8 circuit pack faceplate/pluggable transmission module and the OMD circuit pack (if equipped), the LGX panel, or equivalent connection point for faulty connections or damage.

If faulty connections or damage was...	Then...
found,	Follow local procedures to repair/replace as necessary. Then continue with the next step.
not found,	Proceed to Step 7.

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inc. ODU2/OTU2` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

7 Follow local procedures to measure the incoming optical receive power/wavelength of the affected OTU2 port and compare to office records.

If faulty measurements were...	Then...
found,	Follow local procedures to isolate/clear the upstream trouble. Then continue with the next step.
not found,	Proceed to Step 10.

8 From the System View, click the **Alarm List** button and click **Refresh**.

9 Is the `inc. ODU2/OTU2` alarm still present?

If...	Then...
Yes	Continue with the next step.

If...	**Then...**
No	STOP! End of Procedure.

10 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local pluggable transmission module.

Reference: Procedure 6-8: “Replace pluggable transmission module” (p. 6-71)

11 From the System View, click the **Alarm List** button and click **Refresh**.

12 Is the `inc. ODU2/OTU2` alarm still present?

If...	**Then...**
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

13 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local XM10G/8 circuit pack.

Reference: Procedure 6-29: "Replace 10G Muxponder circuit pack" (p. 6-296)

14 From the System View, click the **Alarm List** button and click **Refresh**.

15 Is the `inc. ODU2/OTU2` alarm still present?

If...	Then...
Yes	Remove the replacement circuit pack and return the original circuit pack to the slot, then continue with the next step.
No	STOP! End of Procedure.

16 **Important!** At this point, the local network element is operating correctly. The trouble is in the far-end network element or in the network between the far-end network element and the local network element.

Follow local procedures for addressing conditions/alarms at the far-end network element.

17 From the System View at the local network element, click the **Alarm List** button and click **Refresh**.

18 Is the `inc. ODU2/OTU2` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

19 Follow local procedures to isolate and clear the network trouble between the far-end network element and the local network element.

END OF STEPS

Procedure 5-72: Clear "inc. OTS LOS-P" alarm

Overview

This procedure is used to clear the `inc. OTS LOS-P` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear `inc. OTS LOS-P` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. OTS LOS-P` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected OTS line, and note the corresponding AID.

3 Visually check the local receive fiber connections between the circuit pack faceplate and the LGX panel or equivalent connection point for faulty connections or damage.

If faulty connections or damage...	Then...
was found,	Follow local procedures to repair/replace as necessary. Then continue with the next step.
was *not* found,	Proceed to Step 6.

4 From the System View, click the **Alarm List** button and click **Refresh**.

5 Is the `inc. OTS LOS-P` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

6 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local OMD circuit pack.

Reference: Procedure 6-28: "Replace DWDM optical multiplexer/demultiplexer circuit pack" (p. 6-294)

7 From the System View, click the **Alarm List** button and click **Refresh**.

8 Is the `inc. OTS LOS-P` alarm still present?

If...	Then...
Yes	Remove the replacement circuit pack and return the original circuit pack to the slot, then continue with the next step.
No	STOP! End of Procedure.

9 **Important!** At this point, the local network element is operating correctly. The trouble is in the far-end network element or in the fiber/cable between the far-end network element and the local network element.

Follow local procedures for addressing OTS-related conditions/alarms at the far-end network element.

10 From the System View at the local network element, click the **Alarm List** button and click **Refresh**.

11 Is the `inc. OTS LOS-P` alarm still present?

If...	**Then...**
Yes	Follow local procedures to isolate and clear the fiber/cable trouble between the far-end network element and the local network element.
No	STOP! End of Procedure.

END OF STEPS

Procedure 5-73: Clear "inc. section trace identifier mismatch" alarms

Overview

This procedure is used to clear the following alarms:

- `inc. EC1 section trace identifier mismatch`
- `inc. EC1 section trace identifier mismatch, diagnostic`
- `inc. OCN section trace identifier mismatch`
- `inc. OCN section trace identifier mismatch, diagnostic`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Obtain office records showing the correct values for the local *Expected Receive Section Trace Format* and *Expected Receive Section Trace Value* parameters.

Steps

Complete the following steps to clear an `inc. section trace identifier mismatch` alarm.

---

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. section trace identifier mismatch` alarm in the resulting Alarm List and note the corresponding AID.

---

2 **Important!** A mismatch exists between the actual *Incoming Receive Section Trace Format/Value* and the provisioned *Expected Receive Section Trace Format/Value*.

Select **View** → **Equipment** to access to the required circuit pack with the affected port. Expand the equipment list by clicking on the plus (+) sign next to the required circuit pack. Click (highlight) the affected port, then click **Select** at the bottom of the window.

Result: The port parameters appear.

---

3 Click the *J0 Section Trace* tab.

Result: The port J0 section trace parameters appear.

4 Record the provisioned *Expected Receive Section Trace Format* and *Expected Receive Section Trace Value* parameters. Click **Close**.

5 Using office records and local procedures, determine if the local *Expected Receive Section Trace Format* and *Expected Receive Section Trace Value* parameters are provisioned correctly.

6 Are the local *Expected Receive Section Trace Format* and *Expected Receive Section Trace Value* parameters provisioned correctly?

If ...	Then...
No,	Select **Configuration** → **Equipment** to access the required port and provision the *Expected Receive Section Trace Format* and/or *Expected Receive Section Trace Value* parameters with the correct values. Then continue with Step 7. **Reference:** *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*
Yes,	Then proceed to Step 9.

7 From the System View, click the **Alarm List** button and click **Refresh**.

8 Is the `inc. section trace identifier mismatch` alarm still present?

If...	Then...
Yes	Continue with Step 9.
No	STOP! End of Procedure.

9 Using local procedures, notify personnel at the site supplying the signal to verify/change the *Transmit Section Trace Format* and/or *Transmit Section Trace Value* parameters as required.

10 From the System View, click the **Alarm List** button and click **Refresh**.

11 Is the `inc. section trace identifier mismatch` alarm still present?

If...	Then...
Yes	Continue with Step 12.
No	STOP! End of Procedure.

12 **Important!** A likely cause of the `inc. section trace identifier mismatch` alarm at the local network element is a mis-connection or a problem with the cabling/wiring between systems.

Follow local procedures to isolate and clear the trouble.

END OF STEPS

Procedure 5-74: Clear "inc. STSN" conditions/alarms

Overview

This procedure is used to clear all `inc. STSN` conditions/alarms, including:

- `inc. STSN AIS`
- `inc. STSN LOP`
- `inc. STSN RFI-P`
- `inc. STSN sig. degrade (BER)`
- `inc. STSN sig. failed (BER)`
- `inc. STSN unequipped`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. STSN` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. STSN` alarm in the resulting alarm list.

2 Determine the alarm level(s) for the active `inc. STSN` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding AID.

4 Note the source address of the STSN alarm/condition reported (for example, m1-1-1). Based on the circuit layout or other office records, determine the other shelf where that time slot is originated (for example, cross-connected to a DS1 or DS3 termination).

5 Log in to the originating shelf.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

6 From the System View, select the **View** → **Cross-Connections**.

7 Are there incomplete or incorrect cross-connections?

If...	Then...
Yes	Continue with Step 8.
No	Proceed to Step 11.

8 From the System View, select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and perform the required provisioning.

9 From the System View, click the **Alarm List** button and click **Refresh**.

10 Is the `inc. STSN` alarm still present?

If...	Then...
Yes	Continue with Step 11.
No	STOP! End of Procedure.

11 One at a time, log in to every shelf where pass-through cross-connections exist for the service (for example, m1-1-1 to m2-1-1 for STS-N). Select the **View** → **Cross-Connections** command from the System View at each shelf to determine if the time slot identified in Step 4 is cross-connected as specified in circuit layout or other office records.

12 At any shelves with missing cross-connections, select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and provision the correct pass-through cross-connection (for example, m1-1-1 to m2-1-1 for STS-N).

13 From the System View, click the **Alarm List** button and click **Refresh**.

14 Is the `inc. STSN` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

15 Check the optical signal level and clean the cable ends if needed. If no problem is found, check the line build-outs (LBOs).

Reference: Procedure 6-11: “Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)” (p. 6-151)

16 From the System View, click the **Alarm List** button and click **Refresh**.

17 Is the `inc. STSN` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

18 Is the OLIU circuit pack equipped with pluggable transmission modules?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 22.

19

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local pluggable transmission module.

Reference: Procedure 6-8: “Replace pluggable transmission module” (p. 6-71)

20 From the System View, click the **Alarm List** button and click **Refresh**.

21 Is the `inc. STSN` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

22

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the terminating OCN OLIU circuit pack.

Reference:

- Procedure 6-5: “Replace high-speed main OLIU circuit pack” (p. 6-48)
- Procedure 6-6: “Replace low-speed function unit OLIU circuit pack” (p. 6-59)

END OF STEPS

Procedure 5-75: Clear "inc. VCG failed" alarm

Overview

This procedure is used to clear an `inc. VCG failed` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. VCG failed` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. VCG failed` alarm in the resulting alarm list.

2 Are there other inc. OCN, STSN, or VT1.5 alarms in the alarm list?

If...	Then...
Yes	Proceed to the appropriate procedure to clear the alarm. Then continue with Step 3.
No	Continue with Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `inc. VCG failed` alarm still present?

If...	Then...
Yes	Continue with Step 5.
No	STOP! End of Procedure.

5 Are there other inc. LOM, inc. SQM, or inc. VCG conditions in the alarm list?

If...	Then...
Yes	Proceed to the appropriate procedure to clear the condition. Then continue with Step 6.
No	Continue with Step 13.

6 From the System View, click the **Alarm List** button and click **Refresh**.

7 Is the `inc. VCG failed` alarm still present?

If...	Then...
Yes	Continue with Step 8.
No	STOP! End of Procedure.

8 From the System View, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

9 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

10 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

11 Log back into the network element. Click the **Alarm List** button and click **Refresh**.

12 Is the `inc. VCG failed` alarm still present?

If...	**Then...**
Yes	Continue with Step 13.
No	STOP! End of Procedure.

13 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding AID.

14 From the System View, select **Fault** → **Reset** → **Smart Pack**. Select the required Ethernet circuit pack and click **Select**. Click **Apply** to reset the circuit pack.

Result: A warning may appear asking you to confirm executing this command. Click **Yes** to reset the smart circuit pack. A dialog box appears indicating a successful reset. Click **OK**.

A smart pack reset may take several minutes to complete depending on the circuit pack type.

15 From the System View, click the **Alarm List** button and click **Refresh**.

16 Is the `inc. VCG failed` alarm still present?

If...	**Then...**
Yes	Continue with Step 17.
No	STOP! End of Procedure.

17 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Perform the following to remove the affected circuit pack completely from the shelf and then re-seat the circuit pack.

1. Release both circuit pack latches.
2. Remove the circuit pack from the shelf, fully disconnecting it from the backplane and removing power. The **ACTIVE** and **FAULT** LEDs extinguish.
3. Re-seat the circuit pack in the shelf and wait approximately 5 minutes.

18 From the System View, click the **Alarm List** button and click **Refresh**.

19 Is the `inc. VCG failed` alarm still present?

If...	Then...
Yes	Continue with Step 20.
No	STOP! End of Procedure.

20

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the near-end Ethernet circuit pack.

Reference: Procedure 6-7: "Replace Ethernet/Data circuit pack" (p. 6-68)

21 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inc. VCG failed` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-76: Clear "inc. VCG LFD" condition

Overview

This procedure is used to clear an `inc. VCG LFD` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. VCG LFD` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. VCG LFD` condition in the resulting alarm list and note the corresponding AID.

2 Are there `inc. STSN` or `inc. VT` alarms associated with the specified VCG in the alarm list?

If...	Then...
Yes	Proceed to the appropriate procedure to clear the alarms in order of severity. Then continue with the next step.
No	Proceed to Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `inc. VCG LFD` condition still present?

If...	Then...
Yes	Continue with Step 5.
No	STOP! End of Procedure.

5 From the System View menu, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

6 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

7 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

8 Log back into the network element. Click the **Alarm List** button and click **Refresh**.

9 Is the `inc. VCG LFD` condition still present?

If...	Then...
Yes	Continue with Step 10.
No	STOP! End of Procedure.

10 **Important!** The Ethernet circuit packs at both terminating network elements must support standard Generic Framing Procedure (GFP) encapsulation (ITU G.7041) for Ethernet over SONET mapping.

Using office records, verify that the affected circuit packs at both terminating network elements support standard Generic Framing Procedure (GFP) encapsulation (ITU G.7041).

If required, replace the affected near-end or far-end circuit pack.

Reference: Procedure 6-7: "Replace Ethernet/Data circuit pack" (p. 6-68)

11 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inc. VCG LFD` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-77: Clear "inc. VCG LOA" condition

Overview

This procedure is used to clear an `inc. VCG LOA` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. VCG LOA` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `inc. VCG LOA` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding AID.

3 **Important!** A tributary may be disabled at the far end SONET network element.

Using office records, determine the far end network element in the SONET network. From the System View menu at the far end SONET network element, select **View** → **Equipment** to access the required VCG tributary and verify that the VCG Membership is Enabled in the Input Direction and Output Direction.

If required, select **Configure** → **Equipment** to access the required VCG tributary and Enable VCG Membership in the Input Direction and/or Output Direction.

4 From the System View, click the **Alarm List** button and click **Refresh**.

5 Is the `inc. VCG LOA` condition still present?

If...	Then...
Yes	Continue with the next step.

If...	Then...
No	STOP! End of Procedure.

6 **Important!** Because the individual tributaries of a VCG can take different paths through the SONET network, they may experience different delays through the network. VCGs use differential delay buffers to accommodate for differential delay.

Follow local procedures to reengineer the circuit path of the affected tributary through the SONET network to reduce differential delay.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) Applications and Planning Guide, 365-372-300*

Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301

7 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inc. VCG LOA` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-78: Clear "inc. VC" conditions/alarms

Overview

This procedure is used to clear all `inc. VC` conditions/alarms, including:

- `inc. VC TU-AIS`
- `inc. VC TU-LOP`
- `inc. VC LP-RFI`
- `inc. VC unequipped`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. VC` condition/alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inc. VC` alarm in the resulting alarm list.

2 Determine the alarm level(s) for the active `inc. VC` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding AID.

4 Note the source address of the VC alarm/condition reported (for example, m1-1-1-1-1). Based on the circuit layout or other office records, determine the other shelf where that time slot is supposed to be originated (cross-connected to a E1 termination).

5 Log in to the originating shelf.

Reference: Procedure 6-2: “Connect Personal Computer (PC) and establish *WaveStar®* CIT session” (p. 6-27)

6 From the System View, select the **View** → **Cross-Connections**.

7 Are there incomplete or incorrect cross-connections?

If...	Then...
Yes	Continue with Step 8.
No	Proceed to Step 11.

8 From the System View, select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and perform the required provisioning.

9 From the System View, click the **Alarm List** button and click **Refresh**.

10 Is the `inc. VC` condition/alarm still present?

If...	Then...
Yes	Continue with Step 11.
No	STOP! End of Procedure.

11 **Important!** At pass-through nodes, all VCs that originate/terminate at the same circuit pack are cross-connected within a single STS3 cross-connection (for example, m1-1-1 to m2-1-1).

One at a time, log in to every shelf where pass-through cross-connections exist for the service. Select the **View** → **Cross-Connections** command from the System View at each shelf to determine if the time slot identified in Step 4 is cross-connected as specified in circuit layout or other office records.

12 At any shelves with missing cross-connections, select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and provision the correct pass-through cross-connection (for example, m1-1-1 to m2-1-1 for STS-3).

13 From the System View, click the **Alarm List** button and click **Refresh**.

14 Is the `inc. VC` condition/alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

15 Check the optical signal level and clean the cable ends if needed. If no problem is found, check the line build-outs (LBOs).

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

16 From the System View, click the **Alarm List** button and click **Refresh**.

17 Is the `inc. VC` condition/alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

18 Is the OLIU circuit pack equipped with pluggable transmission modules?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 22.

19 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local pluggable transmission module.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

20 From the System View, click the **Alarm List** button and click **Refresh**.

21 Is the `inc. VC` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

22 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the terminating OCN OLIU circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

END OF STEPS

Procedure 5-79: Clear "inc. VT" conditions/alarms

Overview

This procedure is used to clear all `inc. VT` conditions/alarms, including:

- `inc. VT AIS`
- `inc. VT LOP`
- `inc. VT RFI-V`
- `inc. VT sig. degrade (BER)`
- `inc. VT unequipped`

Important! When upgrading from an LNW39 to an LNW391. a transient `inc. VT AIS` alarm will be declared and spontaneously cleared. No action is necessary.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inc. VT` alarm.

---

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `inc. VT` alarm in the resulting alarm list.

---

2 Determine the alarm level(s) for the active `inc. VT` alarm(s). Clear the alarms in order of severity.

---

3 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding AID.

---

4 Note the source address of the VT alarm/condition reported (for example, m1-1-1-1-1). Based on the circuit layout or other office records, determine the other shelf where that time slot is supposed to be originated (cross-connected to a DS1 termination).

5 Log in to the originating shelf.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

6 From the System View, select the **View** → **Cross-Connections**.

7 Are there incomplete or incorrect cross-connections?

If...	Then...
Yes	Continue with Step 8.
No	Proceed to Step 11.

8 From the System View, select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and perform the required provisioning.

9 From the System View, click the **Alarm List** button and click **Refresh**.

10 Is the `inc. VT` alarm still present?

If...	Then...
Yes	Continue with Step 11.
No	STOP! End of Procedure.

11 One at a time, log in to every shelf where pass-through cross-connections exist for the service (for example, m1-1-1-1-1 to m2-1-1-1-1 for VT1.5). Select the **View** → **Cross-Connections** command from the System View at each shelf to determine if the time slot identified in Step 4 is cross-connected as specified in circuit layout or other office records.

12 At any shelves with missing cross-connections, select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and provision the correct pass-through cross-connection (for example, m1-1-1-1-1 to m2-1-1-1-1 for VT1.5).

13 From the System View, click the **Alarm List** button and click **Refresh**.

14 Is the `inc. VT` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

15 Check the optical signal level and clean the cable ends if needed. If no problem is found, check the line build-outs (LBOs).

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

16 From the System View, click the **Alarm List** button and click **Refresh**.

17 Is the `inc. VT` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

18 Is the OLIU circuit pack equipped with pluggable transmission modules?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 22.

19 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local pluggable transmission module.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

20 From the System View, click the **Alarm List** button and click **Refresh**.

21 Is the `inc. VT` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

22 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the terminating OCN OLIU circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

END OF STEPS

Procedure 5-80: Clear "incoming CRC-4 MFA mismatch" condition

Overview

This procedure is used to clear an `incoming CRC-4 MFA mismatch` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `incoming CRC-4 MFA mismatch` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `incoming CRC-4 MFA mismatch` condition in the resulting Alarm List and note the corresponding AID.

2 To clear the `incoming CRC-4 MFA mismatch` condition, either change the signal format of the incoming E1 signal to CRC-4 or change the signal format parameter of the local E1 port to Frame Alignment Signal according to local procedures.

If changing the signal format of the...	Then...
incoming E1 signal,	notify personnel at the site supplying the E1 signal to change the signal format to CRC-4. STOP! End of Procedure.
local E1 port,	go to the next step.

3 From the System View, select **Configuration** → **Equipment**. Expand the required circuit pack and TUG signals. Select the required E1 port and click **Select**.

Result: The port provisionable parameters appear.

4 Provision the Signal Format parameter of the E1 port to *Frame Alignment Signal* and click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-81: Clear "incompatible CP version" alarm

Overview

This procedure is used to clear a `incompatible CP version` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Laser safety” (p. 1-6) and “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear a `incompatible CP version`alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `incompatible CP version` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding slot AID.

3 **Important!** An older version of the LNW27 OC-48 OLIU circuit pack was inserted into a slot that contained a newer version of the LNW27 OC-48 OLIU circuit pack.

Select **Reports** → **Equipment Lists** → **Pack**. Select *Shelf* and click **Select** to obtain the *Circuit Pack List*. Observe the correct circuit pack version for the required slot.

4 Replace the old version of circuit pack currently in the required slot with the correct version of the circuit pack.

Reference: Procedure 6-5: “Replace high-speed main OLIU circuit pack” (p. 6-48)

END OF STEPS

Procedure 5-82: Clear "Inconsistent APS Codes" alarm

Overview

This procedure is used to clear an `Inconsistent APS Codes` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `Inconsistent APS Codes` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `Inconsistent APS Codes` alarm in the resulting Alarm List and note the corresponding AID.

2 Are there also incoming signal, pluggable transmission module, or circuit pack-related alarms/conditions associated with that AID?

If...	Then...
Yes	Proceed to the appropriate procedures to clear the alarms in order of severity. Then continue with the next step.
No	Proceed to Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `Inconsistent APS Codes` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

5 Check optical connections for the presence of an incoming signal and measure the optical signal level. Clean the cable ends if needed. If no problem is found, check the line build-outs (LBOs).

Reference: Procedure 6-11: “Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)” (p. 6-151)

6 From the System View, click the **Alarm List** button and click **Refresh**.

7 Is the `Inconsistent APS Codes` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

8 Are the near-end and the far-end OLIU circuit packs equipped with pluggable transmission modules?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 12.

9

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected near-end and then the far-end pluggable transmission module.

Reference: Procedure 6-8: “Replace pluggable transmission module” (p. 6-71)

10 From the System View, click the **Alarm List** button and click **Refresh**.

11 Is the `Inconsistent APS Codes` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

12 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the near-end and then the far-end OLIU circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

13 From the System View, click the **Alarm List** button and click **Refresh**.

14 Is the `Inconsistent APS Codes` alarm still present?

If...	Then...
Yes	Remove the replacement OCn circuit pack and return the original circuit pack to the slot, then continue with the next step.
No	STOP! End of Procedure.

15 Replace the SYSCTL circuit pack.

Reference: Procedure 6-10: “Upgrade or replace SYSCTL (LNW2) circuit pack” (p. 6-99)

16 From the System View, click the **Alarm List** button and click **Refresh**.

If the `Inconsistent APS Codes` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-83: Clear "Inconsistent crs map" alarm

Overview

Use this procedure to clear the `Inconsistent crs map` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Locate the most recent backup copy of the network element database.

Steps

Complete the following steps to clear the `Inconsistent crs map` alarm.

1 Restore the most recent network element database using the **Configuration** → **Software** → **Remote Restore** command.

Reference:

- Procedure 6-21: "Backup and restore NE database via FTP" (p. 6-252)
- Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264)
- Procedure 6-23: "Backup and restore NE database via FTAM" (p. 6-279)

2 When the system reset is complete, log in to the network element.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

END OF STEPS

Procedure 5-84: Clear "inconsistent DCC values" alarm

Overview

This procedure is used to clear an `inconsistent DCC values` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7)in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Obtain office records that specify the correct DCC termination settings for the affected optical span.

Steps

Complete the following steps to clear an `inconsistent DCC values` alarm.

---

1 From the *WaveStar*® CIT System View, click the**Alarm List** button and locate the `inconsistent DCC values` alarm in the resulting Alarm List and note the corresponding AID.

---

2 From the System View, select **View** → **DCC Terminations**.

Result: The *View DCC Terminations* window opens.

---

3 **Important!** The LAPD Role parameter must be provisioned differently at each end of an optical span. For example, if the LAPD Role parameter is provisioned user-side at one end of an optical span, then the LAPD Role parameter must be provisioned network-side at the other end of the optical span.

Does the *OSI over DCC* column read **enabled** AND does the *LAPD Role* column read **use-side** or **network-side** appropriately for the affected DCC ports?

If...	Then...
Yes and the optical span is part of a BLSR,	Proceed to Step 7.
Yes and the optical span is *not* part of a BLSR,	Proceed to Step 9.
No,	Continue with Step 4.

4 From the System View, select **Configuration** → **DCC Terminations** to access the required DCC ports and provision the correct user-side and network-side assignments.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `inconsistent DCC values` alarm still present?

If...	Then...
Yes and the optical span is part of a BLSR,	Continue with Step 7.
Yes and the optical span is *not* part of a BLSR,	Proceed to Step 9.
No	STOP! End of Procedure.

7 From the System View, select **View** → **Ring Map** → **Ring Map**. Select the required ring and click **Select**. Verify that the inactive manual ring map was provisioned correctly.

Result: The *Ring Map* window opens.

8 Is either the West Link or the East Link Isolated?

If...	Then...
Yes	The adjacent node on the corresponding side (East or West) is either being initialized, powered up, powered down. Wait for the node to come up again.
No	Continue with Step 9.

9 From the System View, click the **Alarm List** button and click **Refresh**.

If the `inconsistent DCC values` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-85: Clear "Inconsistent Ring Prot Mode" alarm

Overview

This procedure is used to clear an `Inconsistent Ring Prot Mode` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7)in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `Inconsistent Ring Prot Mode` condition.

1 From the *WaveStar*® CIT System View, click the**Alarm List** button and locate the `Inconsistent Ring Prot Mode` alarm in the resulting Alarm List and note the corresponding AID.

2 At each node in the BLSR, select **View** → **Equipment** to access the ports that interface with the BLSR and verify that the port *Application* parameter is provisioned **2F BLSR**.

If required, select **Configuration** → **Equipment** to access the ports that interface with the BLSR and provision the port *Application* parameter **2F BLSR**.

3 From the System View, click the **Alarm List** button and click **Refresh**.

Important! While the Automatic Ring Discovery (ARD) feature updates the ring map, there will be momentary alarms, such as `Ring Prot Switching Suspended`, `Ring Discovery In Progress`. These alarms will clear automatically when automatic ring discovery completes.

Result: The `Inconsistent Ring Prot Mode` alarm is no longer present.

END OF STEPS

Procedure 5-86: Clear "Inconsistent VT BLSR Access" condition

Overview

This procedure is used to clear an `Inconsistent VT BLSR Access` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7)in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `Inconsistent VT BLSR Access` condition.

1 From the *WaveStar®* CIT System View, click **Alarm List** button and locate the `Inconsistent VT BLSR Access` condition the resulting Alarm List and note the corresponding AID.

2 To clear the `Inconsistent VT BLSR Access` condition, either delete the offending cross-connection or provision the Inconsistent VT BLSR Access Alarm Level to Not Reported according to local procedures.

If...	Then...
deleting the offending cross-connection,	Perform the following. 1. From the System View, select **View** → **Cross-Connections**, then click the *Ptn Grp* tab. Select the required 2F BLSR protection group and click **Select**. The *View Cross-Connection* window opens. 2. Identify the VT1.5 add/drop and/or the VT-accessed STS-1 pass through cross-connections. Record the *Source*, *Destination*, and *Rate*, then click **Close**. 3. From the System View, select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and delete the required cross-connection.

If...	Then...
provisioning the Inconsistent VT BLSR Access Alarm Level parameter to Not Reported,	Perform the following. 1. From the System View, select **Configuration** → **Equipment**, then click the *Ptn Grp* tab. Select the required 2F BLSR protection group and click **Select**. The protection group parameters appear. 2. Provision the Inconsistent *VT BLSR Access Alarm Level* to *Not Reported*. Click **Apply** and **Close**.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `Inconsistent VT BLSR Access` condition still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

5 From the System View, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

6 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

7 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

8 Log back into the network element. Click the **Alarm List** button and click **Refresh**.

9 From the System View, click the **Alarm List** button and click **Refresh**.

If the `Inconsistent VT BLSR Access` condition is still present, contact your next level of support.

END OF STEPS

Procedure 5-87: Clear "inhibit switch" condition

Overview

This procedure is used to clear an `inhibit switch` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `inhibit switch` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `inhibit switch` condition in the resulting Alarm List and note the corresponding AID and the Alarm Entity Type.

2

If ...	Then...
External Synchronization References	Use **Fault** → **Timing/Sync Protection Switch** → **System Timing Reference/Source Switch** to perform a **Reset** *Switch Command*.
Equipment Protection Group	Use **Fault** → **Protection Switch** to access the required 1+1 equipment protection group and perform a **Reset** *Switch Type*.

END OF STEPS

Procedure 5-88: Clear "install failed" condition

Overview

This procedure is used to clear the `install failed` condition.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear the `install failed` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `install failed` condition in the resulting alarm list and note the corresponding AID.

2 **Important!** A *Smart* or *Smart, Override Alarms* software apply operation downloads software to the circuit packs that require updates only.

From the System View, select **Configuration** → **Software** → **Apply Software** to schedule a *Smart* or *Smart, Override Alarms* software apply operation.

Result: Approximately 15 minutes after the scheduled Smart apply time, the apply is complete. You will be logged off the system when the system resets.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

Reference: Procedure 6-20: “Apply software generic” (p. 6-249)

3 Log back into the network element. From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `install failed` condition still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

5 From the System View, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

6 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

7 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

8 Log back into the network element. From the System View, click the **Alarm List** button and click **Refresh**.

9 Is the `install failed` condition still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

10 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Perform the following to remove the affected circuit pack completely from the shelf and then re-seat the circuit pack.

1. Release both circuit pack latches.
2. Remove the circuit pack from the shelf, fully disconnecting it from the backplane and removing power. The **ACTIVE** and **FAULT** LEDs extinguish.
3. Re-seat the circuit pack in the shelf and wait approximately 5 minutes.

11 From the System View, click the **Alarm List** button and click **Refresh**.

12 Is the `install failed` condition still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

13 Replace the affected circuit pack.

Reference: Refer to the appropriate circuit pack replacement procedure in Chapter 6, “Supporting procedures”.

14 From the System View, click the **Alarm List** button and click **Refresh**.

If the `install failed` condition is still present, contact your next level of support.

END OF STEPS

Procedure 5-89: Clear "Line Automatic Switch" condition

Overview

This procedure is used to clear a `Line Automatic Switch` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Line Automatic Switch` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Line Automatic Switch` condition in the resulting alarm list and note the corresponding AID.

Important! This condition is reported in response to an automatic protection switch in the BLSR. In order to clear this condition, you must determine and clear the underlying cause of the protection switch. When the causative alarm is cleared and the provisioned Wait-to-Restore (WTR) time passes, the BLSR will revert to its original state and this condition clears.

2 Are there other alarms associated with the affected AID?

If...	Then...
Yes	Proceed to the appropriate procedures and clear all alarms in order of severity. Then continue with the next step.
No	Proceed to Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `Line Automatic Switch` condition still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

5 From office records, determine which network element is at the other end of the switched line.

6 Select **Reports** → **Remote NE Alarm List** to obtain the *Remote NE Alarm List*.

7 Are there any alarms present on the network element at the other end of the switched line?

If...	Then...
Yes	Log in to the network element at the other end of the switched line and clear all alarms in order of severity. Then continue with the next step.
No	Proceed to Step 10.

8 From the System View, click the **Alarm List** button and click **Refresh**.

9 Is the `Line Automatic Switch` condition still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

10 **Important!** When the cause of the automatic line protection switch clears and the provisioned Wait-to-Restore time passes, the BLSR reverts to its original state and this condition clears. If the Wait-to-Restore parameter is provisioned *99* (infinity), line protection switching is nonrevertive and the line protection switch must be cleared.

Select **View** → **Protection** to access the appropriate 2F BLSR Protection Group and determine the provisioned value of the Wait-to-Restore parameter.

If required, select **Fault** → **Protection Switch** to access the appropriate 2F BLSR Protection Group and perform a **Clear** *Switch Type* in the required *Direction*.

END OF STEPS

Procedure 5-90: Clear "line DCC channel failed" alarm

Overview

This procedure is used to clear a `line DCC channel failed` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `line DCC channel failed` alarm.

---

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `line DCC channel failed` alarm in the resulting alarm list and note the corresponding AID.

---

2 Using office records, identify and log in to the far-end SONET network element supplying the optical signal.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

---

3 At the far-end SONET network element, select **Administration** → **Data Communications** to access the *SCN* tab and verify that *IP over Line DCC* is enabled for the affected port.

If required, enable *IP over Line DCC* for the affected port and click **Apply**.

---

4 At the local network element, click the **Alarm List** button and click **Refresh**.

---

5 Is the `line DCC channel failed` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

6 At the local network element, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

7 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

8 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

9 Log back into the local network element. Click the **Alarm List** button and click **Refresh**.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

10 Is the `line DCC channel failed` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

11 At the far-end SONET network element, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

12 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

13 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

14 Log back into the far-end SONET network element.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

15 At the local network element, click the **Alarm List** button and click **Refresh**.

16 Is the `line DCC channel failed` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

17 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

At the far-end SONET network element, replace the affected pluggable transmission module.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

18 At the local network element, click the **Alarm List** button and click **Refresh**.

19 Is the `line DCC channel failed` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

20

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

At the far-end SONET network element, replace the affected OLIU circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

21 At the local network element, click the **Alarm List** button and click **Refresh**.

22 Is the `line DCC channel failed` alarm still present?

If...	Then...
Yes	Remove the replacement OCn circuit pack and return the original circuit pack to the slot, then continue with the next step.
No	STOP! End of Procedure.

23 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

At the local network element, replace the affected pluggable transmission module.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

24 At the local network element, click the **Alarm List** button and click **Refresh**.

25 Is the `line DCC channel failed` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

26 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

At the local network element, replace the affected OLIU circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

27 At the local network element, click the **Alarm List** button and click **Refresh**.

If the `line DCC channel failed` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-91: Clear "lockout of protection" condition

Overview

This procedure is used to clear a `lockout of protection` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `lockout of protection` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `lockout of protection` condition in the resulting alarm list and note the corresponding AID.

2 Select **Fault** → **Protection Switch** to access the appropriate Protection Group and perform a **Clear** *Switch Type*.

END OF STEPS

Procedure 5-92: Clear "Lockout Switch" condition

Overview

This procedure is used to clear a `Lockout Switch` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Lockout Switch` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Lockout Switch` condition in the resulting alarm list and note the corresponding AID.

2 Select **Fault** → **Protection Switch** to access the appropriate 2F BLSR Protection Group and perform a **Clear** *Switch Type* in the required *Direction*.

END OF STEPS

Procedure 5-93: Clear "lockout switching" condition

Overview

This procedure is used to clear a `lockout switching` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `lockout switching` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `lockout switching` condition in the resulting alarm list and note the corresponding AID.

2 Select **Fault** → **Protection Switch** to access the appropriate 1+1_OPTM Protection Group and perform a **Clear** *Switch Type*.

END OF STEPS

Procedure 5-94: Clear "manual reference switch" condition

Overview

This procedure is used to clear a `manual reference switch` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `manual reference switch` condition.

1 From the System View, select **Fault** → **Timing/Sync Protection Switch** → **System Timing Reference/Source Switch**, select **Reset**, and click **OK**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes**.

2 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `manual reference switch` condition is no longer present.

END OF STEPS

Procedure 5-95: Clear "manual switch" condition

Overview

This procedure is used to clear a `manual switch` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `manual switch` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `manual switch` condition in the resulting alarm list and note the corresponding AID and the Alarm Entity Type.

2 Is the alarmed AID an external synchronization reference?

If...	Then...
Yes	Continue with Step 3.
No	Proceed to Step 4.

3 From the System View, select **Fault** → **Timing/Sync Protection Switch** → **System Timing Reference/Source Switch**, select **Reset**, and click **OK**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes**.

STOP! End of Procedure.

4 From the System View, select **Fault** → **Protection Switch**, highlight the affected Protection Group, and then click **Select**.

Result: On the right side of the *Switch Protection* window, the Switch Type: pull-down menu appears.

5 From the Switch Type: pull-down menu, select **Reset** and click **Apply**.

Result: A warning message appears asking you to confirm executing this command.

6 Click **Yes** to release the manual switch. Click **Close** on the Switch Protection window.

END OF STEPS

Procedure 5-96: Clear "Manual Switch" condition

Overview

This procedure is used to clear a `Manual Switch` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Manual Switch` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Manual Switch` condition in the resulting alarm list and note the corresponding AID.

2 Select **Fault** → **Protection Switch** to access the appropriate 2F BLSR Protection Group and perform a **Clear** *Switch Type* in the required *Direction*.

END OF STEPS

Procedure 5-97: Clear "manual sync. mode switch" condition

Overview

This procedure is used to clear a `manual sync. mode switch` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `manual sync. mode switch` condition.

1 From the System View, select **Fault** → **Timing/Sync Protection Switch** → **Clock Mode Switch**, select **Norm**, and click **OK**.

2 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `manual sync. mode switch` condition is no longer present.

END OF STEPS

Procedure 5-98: Clear "Member Not Collecting/Distributing" alarm

Overview

This procedure is used to clear a `Member Not Collecting/Distributing` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Member Not Collecting/Distributing` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Member Not Collecting/Distributing` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected LAN port, and note the corresponding LAN port AID.

3 **Important!** A likely cause of the `Member Not Collecting/Distributing` alarm at the local network element is a configuration conflict with the interfacing customer LAN port (LAG partner). The Link Aggregation Group and/or LAN port provisioning at the interfacing customer equipment is incompatible.

Follow local procedures for addressing configuration conflicts at the interfacing customer equipment.

4 From the System View, click the **Alarm List** button and click **Refresh**.

5 Is the `Member Not Collecting/Distributing` alarm still present?

If...	Then...
Yes	Continue with the next step.

If...	Then...
No	STOP! End of Procedure.

6 From the System View menu, select **Configuration** → **Data** → **Create/Modify/Delete LA Group** to access the required local Link Aggregation Group and provision the *Protocol* parameter to **None** to disable the Link Aggregation Control Protocol and enable forced aggregation.

7 From the System View, click the **Alarm List** button and click **Refresh**.

If the `Member Not Collecting/Distributing` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-99: Clear "Member Signal Unacceptable - LCAS" alarm

Overview

This procedure is used to clear a `Member Signal Unacceptable-LCAS` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Member Signal Unacceptable-LCAS` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `Member Signal Unacceptable-LCAS` alarm in the resulting alarm list.

2 From the System View, select **Reports** → **NE History Log**. Then click **Retrieve all** and **OK** to obtain the *NE History Log*.

3 Are there `inc. LOM` conditions in the *NE History Log*?

If...	Then...
Yes	Continue with Step 4.

If...	Then...
No	**Important!** Because the individual tributaries of a VCG can take different paths through the SONET network, they may experience different delays through the network. VCGs use differential delay buffers to accommodate for differential delay. Follow local procedures to reengineer the circuit path of the affected tributary through the SONET network to reduce differential delay. (Refer to *Alcatel-Lucent 1665 Data Multiplexer (DMX) Applications and Planning Guide, 365-372-300* and *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.) Then proceed to Step 14.

4 Refer to the *NE History Log* and determine the circuit pack is affected by the `inc. LOM` condition and note the corresponding tributary AID.

5 Using circuit layouts and/or other office records, determine the circuit path through the network and other network element where the VT1.5/STS-n timeslot is terminated.

6 Log in to the other terminating network element.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

7 From the System View, select **View** → **Cross-Connections** to obtain cross-connection information for the required circuit.

8 Are there incomplete or incorrect cross-connections?

If...	Then...
Yes	Continue with Step 9.
No	Proceed to Step 12.

9 From the System View, select **Configuration** → **Cross-Connections** and use the *Cross-Connection Wizard* to provision the cross-connections as required.

10 From the System View, click the **Alarm List** button and click **Refresh**.

11 Is the `Member Signal Unacceptable-LCAS` alarm still present?

If...	Then...
Yes	Continue with Step 12.
No	STOP! End of Procedure.

12 One at a time, log in to every network element that the circuit passes through. Select the **View** → **Cross-Connections** command from the System View at each network element to determine if the time slot identified in Step 4 is cross-connected as specified in circuit layout or other office records.

13 At any shelves with missing cross-connections, select **Configuration** → **Cross-Connections** and use the *Cross-Connection Wizard* to provision the required pass-through cross-connections.

14 From the System View, click the **Alarm List** button and click **Refresh**.

15 Is the `Member Signal Unacceptable-LCAS` alarm still present?

If...	Then...
Yes	Continue with Step 16.
No	STOP! End of Procedure.

16 From the System View, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

---

17 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

---

18 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

---

19 Log back into the network element. Click the **Alarm List** button and click **Refresh**.

---

20 Is the `Member Signal Unacceptable-LCAS` alarm still present?

If...	Then...
Yes	Continue with Step 21.
No	STOP! End of Procedure.

---

21 Replace the Ethernet circuit pack.

Reference: Procedure 6-7: "Replace Ethernet/Data circuit pack" (p. 6-68)

---

22 From the System View, click the **Alarm List** button and click **Refresh**.

If the `Member Signal Unacceptable-LCAS` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-100: Clear "neighbor SYSCTL CP unavailable (nbr tid = TID)" alarm

Overview

This procedure is used to clear a `neighbor SYSCTL CP unavailable (nbr tid = TID)` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `neighbor SYSCTL CP unavailable (nbr tid = TID)` alarm.

---

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `neighbor SYSCTL CP unavailable (nbr tid = TID)` alarm and the `section DCC failed` alarm in the resulting alarm list.

---

2 Refer to the Probable Cause column in the alarm list, determine the affected the circuit pack, and note the corresponding AID.

---

3 Refer to the Description column in the alarm list, and note the nbr tid = TID (neighbor target identifier = LT-DMX [default]).

> **Important!** If the nbr tid = UNKNOWN, consult your network diagrams and/or local procedures and determine the TID of the remote node that is connected to the affected OLIU.

---

4 Log in to the neighboring NE (using its TID) via TCP/IP or OSI or dispatch local craft to the remote site and login serially.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

5 Are you successfully logged into the remote shelf?

If...	Then...
Yes	Continue with Step 6.
No	The remote/neighbor SYSCTL is failed. Proceed to Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99).

6 From the System View of the remote shelf, click the **Alarm List** button.

7 Is there `section DCC channel failed` alarm or `inc. OCN` alarm present?

If...	Then...
Yes	Proceed to Procedure 5-130: "Clear "section DCC channel failed" alarm" (p. 5-317) Or Procedure 5-68: "Clear "inc. OCN" alarms" (p. 5-176) Then continue with Step 8.
No	Proceed to Step 10.

8 From the System View of the remote NE, click the **Alarm List** button and click **Refresh**.

9 Is the `section DCC channel failed` alarm or the inc. OCN alarm(s) still present?

If...	Then...
Yes	Contact your next level of support.
No	Continue with Step 10.

10 From the System View of the local NE (the NE indicating the `neighbor SYSCTL CP unavailable (nbr tid = TID)` alarm), click the **Alarm List** button and click **Refresh**.

11 Is the `neighbor SYSCTL CP unavailable (nbr tid = TID)` or the `section DCC channel failed` alarm still present?

If...	Then...
Yes	Contact your next level of support.
No	STOP! End of Procedure.

END OF STEPS

Procedure 5-101: Clear "Node ID Mismatch" alarm

Overview

This procedure is used to clear a `Node ID Mismatch` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Node ID Mismatch` alarm.

1 Is there a `Default K-bytes` alarm present?

If...	Then...
Yes	Proceed to Procedure 5-19: "Clear "Default K-bytes" alarm" (p. 5-58). Then continue with the next step.
No	Continue with Step 4.

2 From the System View, click the **Alarm List** button and click **Refresh**.

3 Is the `Node ID Mismatch` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

4 **Important!** The port Application parameter of the OC-N ports that interface with the BLSR must be provisioned *2F BLSR*.

At each node in the BLSR, use **View** → **Equipment** to access the required OC-N ports and verify that the port Application parameter is provisioned *2F BLSR*.

If required, use **Configuration** → **Equipment** to access the required OC-N ports and provision the port Application parameter *2F BLSR*.

5 From the System View, select **View** → **Protection** and click the **Ptn Grp** tab, select the appropriate 2F BLSR Protection Group, and click **Select**.

Result: The *View Protection* window opens.

6 From the *View Protection* window, select the **Provisionable Parameters** tab.

7 Is Automatic Ring Discovery either enabled or disabled on all nodes in the ring?

If...	Then...
Yes	Proceed to Step 11.
No	Continue with Step 8 to provision all nodes in the ring in the same manner.

8 From the System View, select **Configuration** → **Equipment** and the **Ptn Grp** tab, select the appropriate 2F BLSR Protection Group, and click **Select**.

Result: The *Configure Equipment* window opens.

9 From the *Configure Equipment* window, select the provisioning you want for Automatic Ring Discovery on your ring, either **Enabled** or **Disabled**. Click **Apply** and **Close**.

10 Repeat Step 8 and Step 9 for all nodes in the ring.

11 Did you enable Automatic Ring Discovery?

If...	Then...
Yes	Continue with Step 12.
No	Proceed to Step 15.

12 From the System View, click the **Alarm List** button and click **Refresh**.

Result: `Ring Discovery In Progress` condition is present. Wait for the discovery to complete.

13 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `Node ID Mismatch` alarm and the `Ring Discovery In Progress` condition are no longer present.

14 Are there any other alarms listed?

If...	Then...
Yes	Proceed to the appropriate procedure to clear the alarm.
No	STOP! End of Procedure.

15 Select **Configuration** → **Configure Manual Ring Map**

Result: The *Configure Manual Ring Map* window opens.

16 Select the required Ring ID and click **Select**.

Result: The *Configure Manual Ring* window opens.

17 Right-click on the node that you wish to modify with a different Node ID.

Result: The *Manual Ring - Modified Existing Ring Node* window opens.

18 Enter the **Modified Node ID** and click **OK**.

Result: A confirmation window opens.

19 Click **Yes** and then click **Apply** in the *Configure Manual Ring* screen.

20 Select **View** → **Ring Map** → **Ring Map**. Select the required Ring ID and click **Select**. Verify that the inactive manual ring map was provisioned correctly and click **Close**.

21 Select **Configuration** → **Activate Manual Ring Map**

Result: The *Apply Manual Ring Map* window opens.

22 Select the required Ring ID and click **Select**.

Result: A dialog box appears asking you to confirm activating the manual ring map. Click **OK**. The inactive manual ring map is now activated.

23 From the System View, select **Reports** → **Remote NE Alarm List**.

Result: The *Remote NE Alarm List* appears.

24 Are there any alarms present on the remote NEs?

If...	Then...
Yes	Log in to the remote NE and clear all alarms in order of severity and then continue with Step 25.
No	Continue with Step 25.

25 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `Node ID Mismatch` alarm is no longer present.

END OF STEPS

Procedure 5-102: Clear "NSAP count in L1 overflowed" alarm

Overview

This procedure is used to clear an `NSAP count in L1 overflowed` alarm.

Before you begin

Prior to performing this procedure, refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.

Steps

Complete the following steps to clear an `NSAP count in L1 overflowed` alarm.

1 Re-engineer the leve1 1 routing area as required to drop the NSAP count to or below 250 nodes.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) Applications and Planning Guide, 365-372-300*

2 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `NSAP count in L1 overflowed` alarm is no longer present.

END OF STEPS

Procedure 5-103: Clear "NSAP count in L1 threshold crossed" alarm

Overview

This procedure is used to clear an `NSAP count in L1 threshold crossed` alarm.

Before you begin

Prior to performing this procedure, refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.

Steps

Complete the following steps to clear an `NSAP count in L1 threshold crossed` alarm.

1 Select **Administration** → **Data Communications** to access the *NSAP Threshold Alarming* tab and disable/reprovision the *Threshold level*,

OR

Re-engineer the leve1 1 routing area as required to drop the NSAP count to or below the provisioned threshold.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) Applications and Planning Guide, 365-372-300*

2 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `NSAP count in L1 threshold crossed` alarm is no longer present.

END OF STEPS

Procedure 5-104: Clear "NTP server(s) unreachable" condition

Overview

This procedure is used to clear an `NTP server(s) unreachable` condition.

Before you begin

Prior to performing this procedure, refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.

Steps

Complete the following steps to clear a `NTP server(s) unreachable` condition.

1 In the System View, select **Administration** → **View Network Time Protocol** to obtain the provisioned *Network Time Protocol Server* information.

2 Verify that *NTP Status* is ENABLED and that a provisioned NTP server is available.

If required, use office records and **Administration** → **Set Network Time Protocol** to make the required provisioning changes.

3 If required, consult and follow local procedures to restore access to an NTP server.

END OF STEPS

Procedure 5-105: Clear "NUT Inconsistent XC Granularity" alarm

Overview

This procedure is used to clear a `NUT Inconsistent XC Granularity` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to identify and clear a `NUT Inconsistent XC Granularity` alarm.

---

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `NUT Inconsistent XC Granularity` alarm in the resulting alarm list and note the corresponding AID.

---

2 From the System View, select **View** → **Cross-Connections** and locate the provisioned cross-connection rate for the alarmed AID.

---

3 From the System View, select **Configuration** → **Equipment**, select the Ptn Grp tab, highlight the 2F BLSR and click **Select**.

Result: The *Configure Equipment* window opens.

---

4 In Local NUT section of the *Configure Equipment* window, click the **View NUT**.

Result: The *View NUT Parameters* window opens.

---

5 In View NUT Parameters window, click the **ALL** button and locate the alarmed cross-connected AID and all its associated tributaries.

6 Identify any and all inconsistencies in the operational NUT (NUT Type column = OPER) for that cross-connection's tributaries and note the TID for the Requesting Node(s). In the View NUT Parameters and the Provision Parameters for Equipment window, click **Close**.

7 Log in to a remote NE with the inconsistency, as determined in Step 6.

8 From the System View, select **Configuration** → **Equipment**, select the Ptn Grp tab, highlight the 2F BLSR and click **Select**.

Result: The *Configure Equipment* window opens.

9 In Local NUT section of the *Configure Equipment* window, change the local NUT provisioning for the alarmed cross-connection to match the other tributaries. Then click **Apply** and **Close**.

Important! For NUT Protection Attribute: Protected = PROT, Not Protected = NOTPR, and Temporary Not Protected = TNOTP.

10 Log back into the original NE with the Local NUT Not operational alarm.

11 From the *WaveStar*® CIT System View, click the **Alarm List** button and click **Refresh**. Is the `NUT Inconsistent XC Granularity` alarm still present?

If...	Then...
Yes	Repeat procedure from Step 7 for another NE with inconstancies.
No	STOP! End of Procedure.

END OF STEPS

Procedure 5-106: Clear "NVM" alarms

Overview

This procedure is used to clear the following alarms:

- `NVM failed`
- `NVM removed or NVM failed`

Important! Performing this procedure under the following scenarios may cause transmission losses and/or require a restore from a remote backup file.

- While the SYSCTL is removed, DO NOT remove or replace either Main circuit pack (M1, M2).
- If an equipped Main (M1 or M2) is removed from the NE, DO NOT replace the SYSCTL.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. If field replacement of NVM modules is allowed, obtain the necessary factory-supplied *replacement* NVM modules.

   Factory-supplied *replacement* NVM modules are correctly formatted; NVMs supplied with an LNW2 have "factory-fresh" software to support maintenance mode.
4. If field replacement of NVM modules is *not* allowed, obtain a replacement LNW2 SYSCTL circuit pack with "factory-fresh" NVM modules.

Steps

Complete the following steps to clear an `NVM`-related alarm.

---

1 From the *WaveStar*® CIT System View,

- Click the **Alarm List** button and locate the `NVM`-related alarm in the resulting alarm list and note the corresponding AID of the failed/missing NVM module.
- Select **View** ⇒ **Software Generic** and record the *Active Generic Release* from the window and the TID from the title bar.

---

2 **Important!** When a failed/missing NVM module is detected, automatic writes to the NVM modules are stopped. Any database changes made after a failed/missing NVM module is detected are stored only in volatile memory.

If field replacement of NVM modules is *not* allowed or if both NVM modules are failed/missing, it is recommended that the network element database be backed up to a remote OS (for example, OMS). This creates a current backup copy of the database that includes all database changes made after a failed/missing NVM module is detected. This backup copy may be used to restore the network element database.

If required, back up the network element database using the **Configuration** → **Software** → **Remote Backup** command.

Reference:

- Procedure 6-21: "Backup and restore NE database via FTP" (p. 6-252)
- Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264)
- Procedure 6-23: "Backup and restore NE database via FTAM" (p. 6-279)

3 **Important!** If field replacement of NVM modules is allowed and only one NVM module is failed/missing, it is recommended that the **OPR-NVM** TL1 command be used to write database changes to the remaining NVM module.

If both NVM modules are failed/missing, the **OPR-NVM** TL1 command is denied. The database changes made after a failed/missing NVM module is detected will not be written on the NVM modules.

If required, perform the following to access the TL1 Cut Through Mode and execute the **OPR-NVM** TL1 command.

1. From the *WaveStar*® CIT System View, select **File** → **NE Disconnect** and click **Yes** in the resulting confirmation window.
2. From the Network View, log back into the NE but this time click **TL1**, not Graphical.
3. Select the *Cut Through Execution Mode* and click **OK**.
4. Enter your user ID and password. Defaults are **LUC01** and **DMX2.5G10G**, respectively.
5. Execute the **OPR-NVM** TL1 command until a `COMPLD` response is received.

   Result: This causes the database changes made after a failed/missing NVM module is detected to be written on the remaining NVM module, if possible.

   Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) TL1 Message Details, 365-372-306*

4 **Important!** If field replacement of NVM modules is allowed, observe the **IND** display on the SYSCTL circuit pack faceplate before removing the SYSCTL circuit pack from the shelf. **N01** indicates the NVM-1 module failed, and **N02** indicates the NVM-2 module failed.

Remove the SYSCTL circuit pack from the shelf.

Reference: Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99)

5

If field replacement of NVM module is...	Then...
allowed, single failed NVM	Obtain the necessary factory-supplied *replacement* NVM module and replace the required failed/missing NVM module in the SYSCTL circuit pack.
double failed NVMs	If both NVMs are replaced with factory-supplied *replacement* NVM modules, the SYSCTL IND displays **E10**. **E10** indicates that there is no software from which to boot. In the case of double failure, refer to Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99).
not allowed,	Obtain a replacement LNW2 SYSCTL circuit pack with factory-fresh NVM modules.

6 Install the SYSCTL circuit pack.

Result: If a valid generic and/or database is *not* found when the SYSCTL circuit pack starts up, the network element enters the Maintenance Mode state and the **IND** display on the SYSCTL circuit pack faceplate shows *MPx.x* (where *x.x* is the generic number).

If in Maintenance Mode, continue with Step 7.

If NOT in Maintenance Mode, proceed to Step 9.

Reference: Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99)

7 **Important!** In the Maintenance Mode state, the default User IDs/passwords must be used to login to the network element. LUC01, LUC02, and LUC03 are the default privileged User IDs, and DMX2.5G10G is the default privileged password.

Log in to the network element.

Result: If the network element is in the Maintenance Mode state, the *Maintenance Mode Wizard* appears.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

8 If required, perform the following to choose/download and install the required valid generic and database using the *Maintenance Mode Wizard*.

1. Follow the *Maintenance Mode Wizard (Screen 1 of 6)* instructions to set the date and time and click **Next**.
2. Follow the *Maintenance Mode Wizard (Screen 2 of 6)* instructions to choose or download the correct generic on the NVM that was not replaced (as noted in Step 1) and click **Next**. Downloading a different generic is not an in-service procedure.
3. Follow the *Maintenance Mode Wizard (Screen 3 of 6)* instructions to verify the TID (as noted in Step 1) and choose or download the current database on the NVM that was not replaced and click **Next**. Selecting the default database will interrupt service.
4. Follow the *Maintenance Mode Wizard (Screen 4 of 6)* instructions to use your selected generic and database and click **Next**.
5. Follow the *Maintenance Mode Wizard (Screen 5 of 6)* instructions to choose a subshelf configuration. and click **Next**.
6. Follow the *Maintenance Mode Wizard (Screen 6 of 6)* instructions and verify that the correct generic, database, and subshelf configuration were selected. Then click **Finish**.

   Note: If the correct generic and current database are chosen, the circuit packs will not experience any downloads or service interruptions.

   Result: The system resets and you are logged off the system.

   A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

   Reference:

- Procedure 6-16: "Ugrade software generic via SFTP" (p. 6-171)
- Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175)
- Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218)
- Procedure 6-18: "Upgrade software generic via FTTD" (p. 6-212)

9 **Important!** If a default database was selected/installed, the default User IDs/passwords must be used to log in to the network element. LUC01, LUC02, and LUC03 are the default privileged User IDs, and DMX2.5G10G is the default privileged password.

If a valid (non-default) database was selected/installed, the provisioned User IDs/passwords may be used to log in to the network element.

If required, log back into the network element when the system reset is complete.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

10 If a default database was selected/installed using the *Maintenance Mode Wizard*, restore the most recent network element database using the **Configuration** → **Software** → **Remote Restore** command.

Reference:

- Procedure 6-21: "Backup and restore NE database via FTP" (p. 6-252)
- Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264)
- Procedure 6-23: "Backup and restore NE database via FTAM" (p. 6-279)

11 From the *WaveStar®* CIT System View, click the **Alarm List** button and click **Refresh**.

Result: The `NVM` alarms are no longer present.

END OF STEPS

Procedure 5-107: Clear "OCN facility loopback" condition

Overview

This procedure is used to clear an `OCN facility loopback` condition. The condition indicates that a user initiated an OC-n Facility Loopback.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `OCN facility loopback` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `OCN facility loopback` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected port, and note the corresponding AID.

3 From the System View, select **Fault** → **Analysis** → **Loopback**, expand the appropriate Optical circuit pack, select the affected port, and then click **Select**.

Result: The *Loopback* window opens

4 From the Loopback screen, select **Facility** and **Release**. Click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-108: Clear "OCN terminal loopback" condition

Overview

This procedure is used to clear an `OCN terminal loopback` condition. The condition indicates that a user initiated an OCN terminal loopback.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `OCN terminal loopback` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `OCN terminal loopback` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the selected port, and note the corresponding AID.

3 From the System View, select **Fault** → **Analysis** → **Loopback**, expand the appropriate Optical circuit pack, select the optical port, and click **Select**.

Result: The *Loopback* window opens.

4 From the Loopback screen, select **Terminal** and **Release**. Click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-109: Clear "Pluggable Transmission Module insufficient maximum rate" alarm

Overview

This procedure is used to clear a `Pluggable Transmission Module insufficient maximum rate` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Pluggable Transmission Module insufficient maximum rate` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Pluggable Transmission Module insufficient maximum rate` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list and note the corresponding socket AID.

3 **Important!** An XFP pluggable transmission module was inserted into a socket that cannot support the port rate.

From the System View, select **View** → **Equipment** to access the affected port and determine the required port rate.

4 Use office records to verify the correct pluggable transmission module/socket/port/circuit pack.

If...	Then...
correct pluggable transmission module was installed in the *wrong* socket/circuit pack,	Perform the following: 1. Remove the pluggable transmission module from the wrong socket/circuit pack and install the pluggable transmission module in the correct socket/circuit pack. (Refer to Procedure 6-8: “Replace pluggable transmission module” (p. 6-71).) 2. Select **Configuration** → **Update System** → **Update Inventory** to update the system equipment list. STOP! End of Procedure.
wrong pluggable transmission module was installed in the *correct* socket/circuit pack,	Perform the following: 1. Replace the wrong pluggable transmission module with the correct pluggable transmission module. (Refer to Procedure 6-8: “Replace pluggable transmission module” (p. 6-71).) 2. Select **Configuration** → **Update System** → **Update Inventory** to update the system equipment list. STOP! End of Procedure.

END OF STEPS

Procedure 5-110: Clear "Pluggable Transmission Module maintenance IP" condition

Overview

This procedure is used to clear a `Pluggable Transmission Module maintenance IP` condition.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Laser safety” (p. 1-6) and “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear a `Pluggable Transmission Module maintenance IP` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Pluggable Transmission Module maintenance IP` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list and note the corresponding socket AID.

3 **Important!** The `Pluggable Transmission Module maintenance IP` condition is reported when the socket Maintenance State parameter is provisioned to *Maint*.

Select **Configuration** → **Equipment** to access the required socket and provision the Maintenance State parameter back to *Normal*.

END OF STEPS

Procedure 5-111: Clear "Pluggable Transmission Module removed" alarm

Overview

This procedure is used to clear an `Pluggable Transmission Module removed` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Pluggable Transmission Module removed` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Pluggable Transmission Module removed` alarm in the resulting alarm list.

2 Determine the alarm level for the `Pluggable Transmission Module removed` alarm. Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, and note the corresponding socket AID.

4 Using office records, determine if the required socket should contain a pluggable transmission module.

5 Do office records show that the required socket should contain a pluggable transmission module?

If...	Then...
Yes,	Obtain the missing pluggable transmission module and install it into the required slot. Refer to the pluggable transmission module installation procedure in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.
No,	Perform the following: 1. Use **View** → **Cross-Connections** to obtain a current list of cross-connections. If required, use **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and delete any cross-connections to the affected pluggable transmission module. 2. Select **Configuration** → **Update System** → **Update All**. A dialog box appears asking you to confirm executing this command. Click **Yes**. This system update clears the `Pluggable Transmission Module removed` alarm.

END OF STEPS

Procedure 5-112: Clear "Path Integrity Failure" alarm

Overview

This procedure is used to clear a `Path Integrity Failure` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to identify and clear a `Path Integrity Failure` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `Path Integrity Failure` alarm in the resulting alarm list and note the corresponding AID.

2 From the System View, select **View** → **Rings** → **Circuit**.

Result: The *View Circuit* window opens.

3 In the *View Circuit* window, locate the PIF (path integrity failure) at some point in the circuit and record the TID of that node. Click **Close** on the *View Circuit* window.

4 Log in to a remote NE with the missing or incorrect cross-connection.

5 From the System View, select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and provision a new (missing) cross-connection in the circuit or to modify the existing cross-connection.

END OF STEPS

Procedure 5-113: Clear "Port administratively disabled" condition

Overview

This procedure is used to clear a `Port administratively disabled` condition. The condition indicates that a user has disabled the Port Administration Control parameter.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Port administratively disabled` condition.

1 From the *WaveStar*® CIT System View, click the Alarm List button and locate the `Port administratively disabled` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 From the System View, select **Configuration** → **Equipment**, expand the appropriate circuit pack, select the required port, and click **Select**.

Result: The port provisionable parameters appear.

4 Provision the *Port Administration Control* parameter as **Enabled** and click **Apply**.

Result: A warning message appears asking you to confirm executing this command. Click **Yes** and **Close**.

END OF STEPS

Procedure 5-114: Clear "Protection switching byte failure" alarm

Overview

This procedure is used to clear a `Protection switching byte failure` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear a `Protection switching byte failure` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `Protection switching byte failure` alarm in the resulting alarm list and note the corresponding AID.

2 Refer to office records to determine the correct provisioning for the port *Application* parameter of the applicable optical port pair. (The port *Application* parameter of the applicable local optical port pair is currently provisioned Bidirectional 1+1 or Optimized 1+1.)

3 To clear the `Protection switching byte failure` alarm either change the port Application parameter of the applicable local port pair or change the port Application parameter of the applicable far-end port pair according to office records and local procedures.

If changing the port Application parameter of the...	Then...
far-end optical port pair,	notify personnel at the site supplying the optical signal to change the port Application parameter according to office records. STOP! End of procedure.
local optical port pair,	go to the next step.

4 From the System View, select **Configuration** → **Equipment** to access the required port and provision the port *Application* parameter according to office records.

END OF STEPS

Procedure 5-115: Clear "Protection switching channel match failure" alarm

Overview

This procedure is used to clear a `Protection switching channel match failure` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Protection switching channel match failure` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `Protection switching channel match failure` alarm in the resulting alarm list and note the corresponding AID.

2 Refer to office records to determine the correct provisioning for the port *Application* parameter of the applicable optical port pair. (The port *Application* parameter of the applicable local optical port pair is currently provisioned Bidirectional 1+1 or Optimized 1+1.)

3 To clear the `Protection switching channel match failure` alarm either change the port Application parameter of the applicable local port pair or change the port Application parameter of the applicable far-end port pair according to office records and local procedures.

If changing the port Application parameter of the...	Then...
far-end optical port pair,	notify personnel at the site supplying the optical signal to change the port Application parameter according to office records. STOP! End of procedure.

If changing the port Application parameter of the...	Then...
local optical port pair,	go to the next step.

4 From the System View, select **Configuration** → **Equipment** to access the required port and provision the port *Application* parameter according to office records.

END OF STEPS

Procedure 5-116: Clear "PROTN Port Failure/Protection CP Input fault" alarms

Overview

This procedure is used to clear the following alarms:

- `Protection CP Input fault`
- `PROTN DS3 Port Failure`
- `PROTN EC1 Port Failure`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `PROTN Port Failure/Protection CP Input fault` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `PROTN Port Failure/Protection CP Input fault` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected port and circuit pack, and note the corresponding AIDs.

3

NOTICE

Service-disruption hazard

Replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected circuit pack.

Reference:

- Procedure 6-3: "Replace DS1 (LNW6/LNW7/LNW8/LNW801) circuit pack" (p. 6-38)
- Procedure 6-4: "Replace DS3/EC-1/TMUX circuit pack" (p. 6-43)

4 From the System View, click the **Alarm List** button and click **Refresh**.

5 Is the `PROTN Port Failure/Protection CP Input fault` alarm still present?

If...	Then...
Yes	Remove the replacement circuit pack and return the original circuit pack to the slot, then continue with Step 6.
No	STOP! End of Procedure.

6 **NOTICE**

Service-disruption hazard

Disconnecting cables may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Check cable connections between the shelf backplane and the local cross-connect panel or equivalent connection point for faulty connections or damage and repair/replace as necessary.

If a visual inspection does not reveal any problems, you may consider making an electrical measurement per local operating instructions.

7 From the System View, click the **Alarm List** button and click **Refresh**.

8 Is the `PROTN Port Failure/Protection CP Input fault` alarm still present?

If...	Then...
Yes	Continue with Step 9.
No	STOP! End of Procedure.

9

If...	Then...
`PROTN DS3 Port Failure`	Determine and record the signal format of the interfacing customer port connected to the alarmed port on the local network element and then continue with Step 10.
`PROTN EC1 Port Failure`	Proceed to Step 14.

10 From the Alcatel-Lucent 1665 DMX System View, select **View** → **Equipment**, expand the pack, highlight the alarmed port, and click **Select**.

11 Compare the signal format of the local port against the information determined about the interfacing customer port. If there are inconsistencies, determine the correct provisioning and correct according to local procedures.

If the local port is provisioned incorrectly, from the System View, select **Configuration** → **Equipment**, expand the pack, highlight the alarmed port, and click **Select**. Provision the Signal Format appropriately, click **Apply**, and then click **Close**.

12 From the System View, click the **Alarm List** button and click **Refresh**.

13 Is the `PROTN Port Failure/Protection CP Input fault` alarm still present?

If...	Then...
Yes	Continue with Step 14.
No	STOP! End of Procedure.

14 **Important!** A likely cause of the `PROTN Port Failure/Protection CP Input fault` alarm at the local network element is a failure at the interfacing customer port or a problem with the cabling/wiring between systems.

Follow local procedures to isolate and clear the trouble.

END OF STEPS

Procedure 5-117: Clear "Receive buffer overflow" condition

Overview

This procedure is used to clear a `Receive buffer overflow` condition. The condition indicates that insufficient SONET bandwidth (not full rate) is provisioned for the specified Data port.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Receive buffer overflow` condition.

1 From the *WaveStar®* CIT System View, click the Alarm List button and locate the `Receive buffer overflow` condition in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 Select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and provision the required additional STSn add/drop cross-connections.

The *ESCON* mode supports only full-rate service requiring a minimum of 4 STS-1s (6 STS-1s may be required for other vendor equipment), or 2 STS3c, or 1 STS12c cross-connections. The Data ports will not carry traffic end-to-end unless the full rate is provisioned.

The *FC-1G* mode supports partial-rate and full-rate service requiring a minimum of 19 STS-1s or 6 STS3c (7 STS-3c may be required for other vendor equipment) cross-connections. The Data ports will carry traffic when end-to-end paths are established in both directions.

The *FC-2G* mode supports partial-rate and full-rate service requiring a minimum of 37 STS-1s (38 STS-1s may be required for other vendor equipment) or 12 STS3c (13 STS-3c may be required for other vendor equipment) cross-connections. The Data ports will carry traffic when end-to-end paths are established in both directions.

The *FICON-1G* mode supports full-rate service requiring a minimum of 19 STS-1s or 6 STS3c (7 STS-3c may be required for other vendor equipment) cross-connections. The Data ports will not carry traffic end-to-end unless the full rate is provisioned.

The *FICON-2G* mode supports full-rate service requiring a minimum of 37 STS-1s (38 STS-1s may be required for other vendor equipment) or 12 STS3c (13 STS-3c may be required for other vendor equipment) cross-connections. The Data ports will not carry traffic end-to-end unless the full rate is provisioned.

4 From the System View, select **View** → **Cross-Connections** to obtain the current list of cross-connections and verify that the proper cross-connections have been made.

END OF STEPS

Procedure 5-118: Clear "Remote client signal failed" alarm

Overview

This procedure is used to clear a `Remote client signal failed` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Remote client signal failed` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `Remote client signal failed` alarm in the resulting alarm list.

2 Are there other inc. OCN, STSN, VT1.5, or VCG alarms in the alarm list?

If...	Then...
Yes	Proceed to the appropriate procedure to clear the alarm. Then continue with Step 3.
No	Continue with Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `Remote client signal failed` alarm still present?

If...	Then...
Yes	Continue with Step 5.
No	STOP! End of Procedure.

5 From the System View at the far-end network element, click the **Alarm List** button. Are there `inc. LOS` or `inc. Loss of Synch` alarms in the alarm list?

If...	**Then...**
Yes	Proceed to the appropriate procedure to clear the alarm. Then continue with Step 6.
No	Proceed to Step 8.

6 From the System View at the near-end network element, click the **Alarm List** button and click **Refresh**.

7 Is the `Remote client signal failed` alarm still present?

If...	**Then...**
Yes	Continue with Step 8.
No	STOP! End of Procedure.

8 From the System View, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

9 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

10 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

11 Log back into the network element. Click the **Alarm List** button and click **Refresh**.

12 Is the `Remote client signal failed` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

13 At the near-end network element, select **Configuration** → **Equipment** to access the required LAN port and disable the *Remote Client Fail* parameter, or repair the incoming signal at the far-end port according to local procedures.

14 From the System View, click the **Alarm List** button and click **Refresh**.

If the `Remote client signal failed` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-119: Clear "Ring Circuit Alarm Suppressed" condition

Overview

This procedure is used to clear a `Ring Circuit Alarm Suppressed` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to identify and clear a `Ring Circuit Alarm Suppressed` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `Ring Circuit Alarm Suppressed` condition in the resulting alarm list and note the corresponding AID.

2 From the System View, select **Configuration** → **Equipment**, select the Ptn Grp tab, highlight the 2F BLSR and click **Select**.

Result: The *Configure Equipment* window opens.

3 In *Configure Equipment* window, change Ring Circuit Alarm Mode to Enabled. Click **Apply** and **Close**.

4 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `Ring Circuit Alarm Suppressed` condition is no longer present.

END OF STEPS

Procedure 5-120: Clear "Ring Ckt Validation Suspended" alarm

Overview

This procedure is used to clear a `Ring Ckt Validation Suspended` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to identify and clear a `Ring Ckt Validation Suspended` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Ring Ckt Validation Suspended` alarm in the resulting alarm list and note the corresponding AID.

2 In the alarm list, are there any `inc. OCN` or BLSR-related alarms present?

If...	Then...
Yes	Proceed to the appropriate procedure to clear each alarm in order of severity. Continue with Step 3.
No	Proceed to Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `Ring Ckt Validation Suspended` alarm still present?

If...	Then...
Yes	Continue with Step 5.
No	STOP! End of Procedure.

5 From the System View, select **Configuration** → **Equipment** and the **Ptn Grp** tab, select the appropriate 2F BLSR Protection Group, and click **Select**.

Result: The *Configure Equipment* window opens.

6 From the *Configure Equipment* window, select **Disabled** for Automatic Ring Discovery. Click **Apply**.

7 From the *Configure Equipment* window, select **Enabled** for Automatic Ring Discovery. Click **Apply** and **Close**.

Important! While the Automatic Ring Discovery (ARD) feature updates the ring map, there will be momentary alarms, such as `Ring Prot Switching Suspended`, `Ring Discovery In Progress`. Theses will clear automatically when the ARD completes.

8 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `Ring Ckt Validation Suspended` alarm is no longer present.

END OF STEPS

Procedure 5-121: Clear "Ring Comm Failure" alarm

Overview

This procedure is used to clear a `Ring Comm Failure` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Obtain office records that specify the DCC termination parameter values for the affected OC-N ports.

Steps

Complete the following steps to clear a `Ring Comm Failure` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Ring Comm Failure` alarm in the resulting alarm list.

2 Is there an `inconsistent DCC values` or `section DCC channel failed` alarm present in the *Alarm List*?

If...	Then...
Yes	Proceed to the appropriate procedure to clear the alarm. Then continue with Step 3.
No	Proceed to Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `Ring Comm Failure` alarm still present?

If...	Then...
Yes	Continue with Step 5.
No	STOP! End of Procedure.

5 Visually check the local receive fiber connections between the circuit pack faceplate and the LGX panel or equivalent connection point for faulty connections or damage.

If faulty connections or damage...	Then...
was found,	Follow local procedures to repair/replace as necessary. Then continue with Step 6.
was *not* found,	Proceed to Step 8.

6 From the System View, click the **Alarm List** button and click **Refresh**.

7 Is the `Ring Comm Failure` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

8 Is the affected OLIU circuit pack equipped with pluggable transmission modules?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 12.

9 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected pluggable transmission module.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

10 From the System View, click the **Alarm List** button and click **Refresh**.

11 Is the `Ring Comm Failure` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

12 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected local OCn OLIU circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

13 From the System View, click the **Alarm List** button and click **Refresh**.

If the `Ring Comm Failure` condition is still present, contact your next level of support.

END OF STEPS

Procedure 5-122: Clear "Ring Incomplete" alarm

Overview

This procedure is used to clear a `Ring Incomplete` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Ring Incomplete` alarm.

1 In the alarm list, are there any `inc. OCN` or `inc. STSN` alarms present?

If...	Then...
Yes	Proceed to the appropriate procedure to clear each alarm in order of severity. Then continue with the next step.
No	Continue with Step 4.

2 From the System View, click the **Alarm List** button and click **Refresh**.

3 Is the `Ring Incomplete` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

4 **Important!** The port Application parameter of the OC-N ports that interface with the BLSR must be provisioned *2F BLSR*.

At each node in the BLSR, use **View** → **Equipment** to access the required OC-N ports and verify that the port Application parameter is provisioned *2F BLSR*.

If required, use **Configuration** → **Equipment** to access the required OC-N ports and provision the port Application parameter *2F BLSR*.

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `Ring Incomplete` alarm still present?

If...	Then...
Yes	Continue with Step 7.
No	STOP! End of Procedure.

7 From the System View, select **View** → **Protection** and the **Ptn Grp** tab, select the appropriate 2F BLSR Protection Group, and click **Select**.

Result: The *View Protection* window opens.

8 From the View Protection window, select the **Provisionable Parameters** tab.

9 Is Automatic Ring Discovery enabled all nodes in the ring?

If...	Then...
Yes	Proceed to Step 13.
No	Continue with Step 10.

10 From the System View, select **Configuration** → **Equipment** and the **Ptn Grp** tab, select the appropriate 2F BLSR Protection Group, and click **Select**.

Result: The protection group parameters appears.

11 From the *Configure Equipment* window, select the provisioning you want for Automatic Ring Discovery on your ring, either **Enabled** or **Disabled**. Click **Apply** and Close.

12 Repeat Step 10 and Step 11 for all nodes in the ring.

13 From the System View, click the **Alarm List** button and click **Refresh**.

14 Is the `Ring Incomplete` alarm still present?

If...	Then...
Yes	Continue with Step 15.
No	STOP! End of Procedure.

15 From the System View, select **Reports** → **Remote NE Alarm List**.

Result: The *Remote NE Alarm List* appears.

16 Are there any alarms present on the remote NEs?

If...	Then...
Yes	Log in to the remote NE and clear all alarms in order of severity and then continue with Step 17.
No	Continue with Step 17.

17 In the alarm list, is there an `inconsistent DCC values` or `section DCC channel failed` alarm?

If...	Then...
Yes	Proceed to the appropriate procedure to clear the alarm. Then continue with the next step.
No	Proceed to Step 20.

18 From the System View, click the **Alarm List** button and click **Refresh**.

19 Is the `Ring Incomplete` alarm still present?

If...	Then...
Yes	Continue with Step 20.
No	STOP! End of Procedure.

20 From the System View, select **View** → **Ring Map** → **Ring Map**. Select the required ring and click **Select**. Verify that the ring map was provisioned correctly.

Result: The *Ring Map* window opens.

21 Is either the West Link or the East Link Isolated?

If...	Then...
Yes	The adjacent node on the corresponding side (East or West) is either being initialized, powered up, powered down. What for the node to come up again.
No	Continue with Step 22.

22 From the System View, click the **Alarm List** button and click **Refresh**.

23 Is the `Ring Incomplete` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

24 Check the optical signal level and clean the cable ends if needed. If no problem is found, check the line build-outs (LBOs).

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

25 From the System View, click the **Alarm List** button and click **Refresh**.

26 Is the `Ring Incomplete` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

27 Are the near-end and the far-end OLIU circuit packs equipped with pluggable transmission modules?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 31.

28

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected near-end and then the far-end pluggable transmission module.

Reference: Procedure 6-8: “Replace pluggable transmission module” (p. 6-71)

29 From the System View, click the **Alarm List** button and click **Refresh**.

30 Is the `Ring Incomplete` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

31

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the near-end and then the far-end OLIU circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

32 From the System View, click the **Alarm List** button and click **Refresh**.

If the `Ring Incomplete` condition is still present, contact your next level of support.

END OF STEPS

Procedure 5-123: Clear "Ring Prot Switching Suspended" alarm

Overview

This procedure is used to clear a `Ring Prot Switching Suspended` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `Ring Prot Switching Suspended` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Ring Prot Switching Suspended` condition in the resulting alarm list and note the corresponding AID.

2 Is there a `Lockout Switch` condition listed?

If...	Then...
Yes	Protection switching on the BLSR has been disabled. Proceed to Procedure 5-92: "Clear "Lockout Switch" condition" (p. 5-244).
No	Continue with Step 3.

3 Is a new node being added to the ring?

If...	Then...
Yes	Wait for Automatic Ring Discovery to complete a valid ring map.
No	Continue with Step 4.

4 From the System View, select **View** → **Ring Map** → **Ring Map**. Select the required ring and click **Select**. Verify that the ring map was provisioned correctly.

Result: The *Ring Map* window opens.

5 Is either the West Link or the East Link Isolated?

If...	Then...
Yes	The adjacent node on the corresponding side (East or West) is either being initialized, powered up, powered down. What for the node to come up again.
No	Continue with Step 6.

6 Clear any BLSR-related alarms or conditions present in the alarm list.

7 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `Ring Prot Switching Suspended` alarm is no longer present.

END OF STEPS

Procedure 5-124: Clear "ring upgrade mode" condition

Overview

This procedure is used to clear a `ring upgrade mode` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear the `ring upgrade mode` condition.

1 Using local procedures, determine if a network upgrade is being performed.

2

If a network upgrade...	Then...
is being performed,	This condition clears when the network upgrade is completed and the network element is manually provisioned back to the Normal mode. STOP! End of Procedure.
is *not* being performed,	From the System View, select **Configuration** → **Normal Mode**. **Result:** A dialog box appears asking you to confirm changing the NE Mode to Normal mode. Click **Yes**. The **ABN** LED is turned off on the SYSCTL circuit pack faceplate and the Ring Upgrade mode is removed from the Alarm List.

END OF STEPS

Procedure 5-125: Clear "RPR Miscabling" condition

Overview

This procedure is used to clear an `RPR Miscabling` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Obtain office records that show the correct ring connections and required cross-connections.

Steps

Complete the following steps to clear the `RPR Miscabling` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `RPR Miscabling` condition in the resulting alarm list and note the corresponding VCG AID.

2 Select **View** → **Cross-Connections**. Expand the required circuit pack details and select the affected VCG port. Click **Select** to obtain a list of cross-connections. Observe the provisioned cross-connections and compare with office records.

3

If the provisioned cross-connections are ...	Then ...
correct,	Proceed to Step 5.
not correct,	Continue with Step 4.

4 Select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard*. Use the *Cross-Connection Wizard* to delete the existing wrong cross-connections and then create the correct new cross-connections according to office records.

STOP! End of Procedure.

5 Using office records, identify and log in to the adjacent node.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

6 Select **View** → **Cross-Connections**. Expand the required circuit pack details and select the affected VCG port. Click **Select** to obtain a list of cross-connections. Observe the provisioned cross-connections and compare with office records.

7 Select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard*. Use the *Cross-Connection Wizard* to delete the existing wrong cross-connections and then create the correct new cross-connections according to office records.

END OF STEPS

Procedure 5-126: Clear "RPR Topology Exceeded Max Stations" condition

Overview

This procedure is used to clear an `RPR Topology Exceeded Max Stations` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear the `RPR Topology Exceeded Max Stations` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `RPR Topology Exceeded Max Stations` condition in the resulting alarm list and note the corresponding VCG AID.

2 **Important!** The number of nodes in the ring has exceeded the maximum of 255 nodes.

Follow local procedures to reengineer the ring to reduce the number of nodes to 255 or less.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*

END OF STEPS

Procedure 5-127: Clear "RPR Topology Inconsistency" condition

Overview

This procedure is used to clear an `RPR Topology Inconsistency` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Obtain office records that show the correct RPR MAC addresses and required cross-connections for the ring.

Steps

Complete the following steps to clear the `RPR Topology Inconsistency` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `RPR Topology Inconsistency` condition in the resulting alarm list and note the corresponding VCG AID.

2 From the System View, select **View** → **Rings** → **Ring Map**. Select the required RPR ring and click **Select**.

Result: The RPR ring map information appears.

3 Observe the *MAC Address* of each node and Ringlet 0 (*R0*) and Ringlet 1 (*R1*) between each node.

4 **Important!** Each LNW78 100/1G-FSR Gigabit Ethernet circuit pack must have a unique MAC address within the ring.

The ring must be bidirectionally symmetric with respect to the RPR MAC addresses as seen on Ringlet 0 and Ringlet 1.

If ...	**Then ...**
duplicate RPR MAC addresses exist within the ring,	Using the ring map and local procedures, identify and replace the duplicate LNW78 100/1G-FSR Gigabit Ethernet circuit pack. **Reference:** Procedure 6-7: "Replace Ethernet/Data circuit pack" (p. 6-68)
ring addresses are not bidirectionally symmetric,	Using local procedures and the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*, reengineer the ring span(s) making sure that each span is connected bidirectionally to its neighbor.

5 From the System View, click the **Alarm List** button and click **Refresh**.

If the `RPR Topology Inconsistency` condition is still present, contact your next level of support.

END OF STEPS

Procedure 5-128: Clear "RPR Topology Map Entry Invalid" condition

Overview

This procedure is used to clear an `RPR Topology Map Entry Invalid` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear the `RPR Topology Map Entry Invalid` condition.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `RPR Topology Map Entry Invalid` condition in the resulting alarm list and note the corresponding VCG AID.

2 From the System View, select **Configuration** → **Equipment**. Expand the required Ethernet circuit pack, select the affected VCG, and click **Select**.

Click the **Timer** tab and increase the *Topology Stability Timer (msec)* according to local procedures. Click **Apply**, read the warning message, then click **Yes** to execute the command.

Click **Close** to exit.

3 From the System View, click the **Alarm List** button and click **Refresh**.

If the `RPR Topology Map Entry Invalid` condition is still present, repeat Step 2 and Step 3.

END OF STEPS

Procedure 5-129: Clear "RPR Topology Unstable" condition

Overview

This procedure is used to clear an `RPR Topology Unstable` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear the `RPR Topology Unstable` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `RPR Topology Unstable` condition in the resulting alarm list and note the corresponding VCG AID.

2 From the System View, select **Reports** → **NE History Log**. Then click **Retrieve all** and **OK** to obtain the *NE History Log*.

3 **Important!** Multiple or repetitive RPR topology changes occurred whose duration exceeded the provisionable VCG *Topology Stability Timer*. RPR Topology changes include protection switches and adding/deleting nodes to/from the ring.

Review the *NE History Log* for any multiple or repetitive RPR topology changes that affect the specified VCG. Using local procedures determine the cause of the RPR topology changes and clear any associated troubles.

If required, increase the VCG *RPR Protection Wait to Restore* and/or *Topology Stability Timer* parameters using the **Configuration** → **Equipment** command.

END OF STEPS

Procedure 5-130: Clear "section DCC channel failed" alarm

Overview

This procedure is used to clear a `section DCC channel failed` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Obtain office records that specify the required DCC termination settings for the affected DCC.

Steps

Complete the following steps to clear a `section DCC channel failed` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `section DCC channel failed` alarm in the resulting alarm list and note the corresponding AID.

2 From the System View, select **View** → **DCC Terminations**.

Result: The *View DCC Terminations* window opens.

3 **Important!** To enable OSI over DCC operation, the OSI over DCC must be enabled and the LAPD Role must be provisioned differently at each end of an optical span. For example, if the LAPD Role is provisioned user-side at one end of an optical span, then the LAPD Role must be provisioned network-side at the other end of the optical span.

Compare the information in the *View DCC Terminations* window with office records. Are the DCC termination parameters provisioned appropriately for the affected DCC port according to office records?

If...	Then...
Yes	Proceed to Step 7.
No	Continue with Step 4.

4 Select **Configuration** → **DCC Terminations** to access the required DCC ports and provision the DCC termination parameters according to office records.

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `section DCC channel failed` alarm still present?

If...	Then...
Yes	Continue with Step 7.
No	STOP! End of Procedure.

7 Check the optical signal level and clean the cable ends if needed. If no problem is found, check the line build-outs (LBOs).

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

8 From the System View, click the **Alarm List** button and click **Refresh**.

9 Is the `section DCC channel failed` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

10 Are the near-end and the far-end OLIU circuit packs equipped with pluggable transmission modules?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 14.

11 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected near-end and then the far-end pluggable transmission module.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

12 From the System View, click the **Alarm List** button and click **Refresh**.

13 Is the `section DCC channel failed` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

14 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the near-end and then the far-end OLIU circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

15 From the System View, click the **Alarm List** button and click **Refresh**.

If the `section DCC channel failed` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-131: Clear "Squelch Map Inconsistent" alarm

Overview

This procedure is used to clear a `Squelch Map Inconsistent` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to identify and clear a `Squelch Map Inconsistent` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Squelch Map Inconsistent` alarm in the resulting alarm list and note the corresponding AID.

2 From the System View, select **View** → **Rings** → **Circuit**.

Result: The *View Circuit* window opens.

3 In the *View Circuit* window, locate the incorrectly provisioned source or destination (loca/locz) at some point in the circuit and record the TID of that node. Click **Close** on the *View Circuit* window.

4 Log in to the NE with the incorrectly provisioned source or destination (loca/locz).

5 From the System View, select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and modify the existing cross-connection.

END OF STEPS

Procedure 5-132: Clear "Squelch Data Unavailable" alarm

Overview

This procedure is used to clear a `Squelch Data Unavailable` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to identify and clear a `Squelch Data Unavailable` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `Squelch Data Unavailable` alarm in the resulting alarm list and note the corresponding AID.

2 Are DCC-related alarms present in the alarm list?

If...	Then...
Yes	Proceed to the appropriate procedure to clear each alarm in order of severity. Then continue with the next step.
No	Proceed to Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `Squelch Data Unavailable` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

5 From the System View, select **Reports** → **Remote NE Alarm List**.

Result: The *Remote NE Alarm List* window opens.

6 Are DCC-related alarms present on the remote network elements?

If...	Then...
Yes	Log in to the remote network element and clear all alarms in order of severity. Then continue with the next step.
No	Proceed to Step 9.

7 From the System View, click the **Alarm List** button and click **Refresh**.

8 Is the `Squelch Data Unavailable` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

9 From the System View, select **View** → **Rings** → **Circuit**.

Result: The *View Circuit* window opens.

10 In the *View Circuit* window, locate missing cross-connections at some point in the circuit and record the TID of that node. Click **Close** on the *View Circuit* window.

11 Log in to a remote NE with the missing or incorrect cross-connection.

12 From the System View, select **Configuration** → **Cross-Connections** to access the *Cross-Connection Wizard* and provision a new (missing) cross-connection in the circuit or to modify the existing cross-connection.

END OF STEPS

Procedure 5-133: Clear "STP autolock port disable" alarm

Overview

This procedure is used to clear an `STP autolock port disable` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `STP autolock port disable` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `STP autolock port disable` alarm in the resulting alarm list and note the corresponding Ethernet LAN port/VCG AID.

2 Look for equipment alarms/conditions affecting the same AID. Proceed to the appropriate procedure to clear those alarms/conditions.

3 **Important!** The `STP autolock port disable` alarm clears for an Ethernet LAN port/link aggregation group when the Port Administration Control or Ethernet Port Spanning Tree Status parameter is Disabled.

The `STP autolock port disable` alarm clears for a VCG when the VCG Spanning Tree Status parameter is Disabled.

Disabling the Spanning Tree Group Autolock parameter also clears the `STP autolock port disable` alarm.

From the System View, select **Configuration** → **Equipment**. Expand the required circuit pack details, select (highlight) the required Ethernet LAN port/VCG, then click **Select**.

Result: The VCG/Port parameters appear.

4 Select the **Spanning Tree** tab and provision the *Spanning Tree Status* parameter as **Disabled**. Click **Apply** and **Close**.

Result: The spanning tree role of the participating port is DISA (Disabled-Administration).

5 Select **View** → **Equipment** to access the required Ethernet LAN port/VCG and verify that the Spanning Tree Status is *Disabled*.

6 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `STP autolock port disable` condition is no longer present.

7 Select **Configuration** → **Equipment**. Expand the required circuit pack details, select (highlight) the required Ethernet LAN port/VCG, then click **Select**.

Result: The VCG/Port parameters appear.

8 Select the **Spanning Tree** tab and provision the *Spanning Tree Status* parameter as **Enabled**. Click **Apply** and **Close**.

Result: The spanning tree reconfigures.

9 Verify that the existing spanning tree configuration is correct.

Reference: Procedure 6-30: “Verify spanning tree configuration” (p. 6-299)

END OF STEPS

Procedure 5-134: Clear "Subshelf Communication Failed” alarm

Overview

This procedure is used to clear a `Subshelf Communication Failed` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear a `Subshelf Communication Failed` alarm.

1 **Important!** The LAN3 connection, identified as DLAN on the back of a shelf, or the control communications link between the main shelf and each subshelf failed.

To support more than one subshelf, the LAN3 port of the main shelf and of each subshelf must be connected to an Ethernet hub capable of supporting 100Mb operation. No special cable is required.

Visually check the control link connections between the shelf backplane DLAN connectors and the Ethernet hub (if equipped) for faulty connections or damage.

If faulty connections or damage was...	Then...
found,	Follow local procedures to repair/replace as necessary. STOP! End of Procedure.
not found,	Continue with the next step.

2

If alarm is reported for...	Then...
a single Subshelf in the multishelf DCS system,	Continue with the next step.
all Subshelves in the multishelf DCS system,	Then proceed to Step 6.

3 **Important!** When the shelf is in the Maintenance Mode state, the **IND** display on the SYSCTL circuit pack faceplate shows *MPx.x* (where *x.x* is the generic number).

If the shelf is in the Maintenance Mode state, the default User IDs/passwords must be used to log in to the shelf. LUC01, LUC02, and LUC03 are the default privileged User IDs, and DMX2.5G10G is the default privileged password.

If required, perform the following to log in to the affected subshelf using the *WaveStar*® CIT TL1 Cut-Tthrough Mode.

1. From the Network View, log into the shelf but this time click **TL1**, not Graphical.
2. Select the *Cut Through Execution Mode* and click **OK**.
3. Enter a default privileged User ID and password. Defaults are **LUC01** and **DMX2.5G10G**, respectively.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) TL1 Message Details, 365-372-306*

4 Execute the **`init-system (phase 3)`** TL1 command to reset the subshelf.

Result: The shelf resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) TL1 Message Details, 365-372-306*

5 **Important!** The provisioned User IDs/passwords must be used to log in to the shelf.

When the reset is complete, log back into the shelf.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

STOP! End of Procedure.

6 Log in to the main shelf using the *WaveStar*® CIT and select **View** → **Equipment** to access each subshelf. Verify that the subshelf information is provisioned correctly.

If required, select **Configuration** → **Equipment** to access the subshelves and reprovision the subshelf information correctly.

7 From the System View, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

8 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

9 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

10 **Important!** The provisioned User IDs/passwords must be used to log in to the shelf.

When the reset is complete, log back into the shelf.

Reference: Procedure 6-2: “Connect Personal Computer (PC) and establish *WaveStar®* CIT session” (p. 6-27)

END OF STEPS

Procedure 5-135: Clear "Subshelf-related" alarms/conditions

Overview

This procedure is used to clear the following subshelf-related alarms/conditions:

- `Invalid Subshelf Configuration`
- `Multiple Main Shelf TIDs`
- `Subshelf Boot Failed`
- `Subshelf Configuration Mismatch`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Obtain office records specifying the required main shelf/subshelf provisioning.
4. Obtain office records specifying the required valid generic.
5. Locate the most recent backup copy of the network element database in case it is necessary to restore the network element database.

Steps

Complete the following steps to clear subshelf-related alarms/conditions.

1 **Important!** When the shelf is in the Maintenance Mode state, the **IND** display on the SYSCTL circuit pack faceplate shows *MPx.x* (where *x.x* is the generic number).

If the shelf is in the Maintenance Mode state, the default User IDs/passwords must be used to log in to the network element. LUC01, LUC02, and LUC03 are the default privileged User IDs, and DMX2.5G10G is the default privileged password.

Perform the following to log in to the shelf using the *WaveStar*® CIT TL1 Cut-Tthrough Mode.

1. From the Network View, log into the shelf but this time click **TL1**, not Graphical.
2. Select the *Cut Through Execution Mode* and click **OK**.
3. Enter a default privileged User ID and password. Defaults are **LUC01** and **DMX2.5G10G**, respectively.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) TL1 Message Details, 365-372-306*

2 Execute the **`rtrv-alm-all`** TL1 command to obtain a list of active alarms.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) TL1 Message Details, 365-372-306*

3 Observe the list of active alarms.

If...	Then...
`Invalid Subshelf Configuration`	Execute the **`canc-user`** TL1 command to exit the *WaveStar*® CIT TL1 Cut-Tthrough Mode, then proceed to Procedure 5-135.1: “Clear "Invalid Subshelf Configuration" alarm” (p. 5-331).
`Multiple Main Shelf TIDs`	Execute the **`canc-user`** TL1 command to exit the *WaveStar*® CIT TL1 Cut-Tthrough Mode, then proceed to Procedure 5-135.2: “Clear "Multiple Main Shelf TIDs" alarm” (p. 5-333).
`Subshelf Boot Failed`	Execute the **`canc-user`** TL1 command to exit the *WaveStar*® CIT TL1 Cut-Tthrough Mode, then proceed to Procedure 5-135.3: “Clear "Subshelf Boot Failed" alarm” (p. 5-335).
`Subshelf Configuration Mismatch`	Proceed to Procedure 5-135.4: “Clear "Subshelf Configuration Mismatch" alarm” (p. 5-337).

END OF STEPS

Procedure 5-135.1: Clear "Invalid Subshelf Configuration" alarm

Steps

Complete the following steps to clear an `Invalid Subshelf Configuration` alarm.

1 **Important!** When the shelf is in the Maintenance Mode state, the **IND** display on the SYSCTL circuit pack faceplate shows *MPx.x* (where *x.x* is the generic number).

If the shelf is in the Maintenance Mode state, the default User IDs/passwords must be used to log in to the shelf. LUC01, LUC02, and LUC03 are the default privileged User IDs, and DMX2.5G10G is the default privileged password.

Log in to the shelf using the *WaveStar*® CIT *Graphical* Mode.

Result: The *Maintenance Mode Wizard (Screen 1 of 6)* appears.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

2 Perform the following to choose the required subshelf configuration file (ssconfig.dat) on both NVMs.

1. Follow the *Maintenance Mode Wizard (Screen 1 of 6)* instructions to set the date and time and click **Next**.
2. Follow the *Maintenance Mode Wizard (Screen 2 of 6)* instructions to choose/download a generic and click **Next**.
3. Follow the *Maintenance Mode Wizard (Screen 3 of 6)* instructions to choose/download a database and click **Next**.
4. Follow the *Maintenance Mode Wizard (Screen 4 of 6)* instructions to use the selected generic and database and click **Next**.
5. Follow the *Maintenance Mode Wizard (Screen 5 of 6)* instructions to choose the *correct* subshelf configuration and click **Next**.
   If the affected shelf is the Main shelf, select the DEFAULT subshelf configuration file (ssconfig.dat) on both NVMs.
   If the affected shelf is a subshelf, re-write the subshelf configuration file (ssconfig.dat) on both NVMs.
6. Follow the *Maintenance Mode Wizard (Screen 6 of 6)* instructions and verify that the *correct* generic, database, and subshelf configuration were selected. Then click **Finish**.

Result: The shelf resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

3 **Important!** The provisioned User IDs/passwords must be used to log in to the shelf.

When the reset is complete, log back into the shelf.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

END OF STEPS

Procedure 5-135.2: Clear "Multiple Main Shelf TIDs" alarm

Steps

Complete the following steps to clear an `Multiple Main Shelf TIDs` alarm.

1 Using local procedures and office records, determine which shelf connected to the LAN3 control communications link has the duplicate TID.

At the shelf with the duplicate TID, select **Administration** → **Set TID** to reprovision the duplicate TID.

2 **Important!** When the shelf is in the Maintenance Mode state, the **IND** display on the SYSCTL circuit pack faceplate shows *MPx.x* (where *x.x* is the generic number).

If the shelf is in the Maintenance Mode state, the default User IDs/passwords must be used to log in to the shelf. LUC01, LUC02, and LUC03 are the default privileged User IDs, and DMX2.5G10G is the default privileged password.

Log in to the shelf using the *WaveStar*® CIT *Graphical* Mode.

Result: The *Maintenance Mode Wizard (Screen 1 of 6)* appears.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

3 Perform the following to verify the generic, database, and subshelf configuration file (ssconfig.dat) on both NVMs, and reset the shelf.

1. Follow the *Maintenance Mode Wizard (Screen 1 of 6)* instructions to set the date and time and click **Next**.
2. Follow the *Maintenance Mode Wizard (Screen 2 of 6)* instructions to choose/download a generic and click **Next**.
3. Follow the *Maintenance Mode Wizard (Screen 3 of 6)* instructions to choose/download a database and click **Next**.
4. Follow the *Maintenance Mode Wizard (Screen 4 of 6)* instructions to use the selected generic and database and click **Next**.
5. Follow the *Maintenance Mode Wizard (Screen 5 of 6)* instructions to choose a subshelf configuration. and click **Next**.
6. Follow the *Maintenance Mode Wizard (Screen 6 of 6)* instructions and verify that the correct generic, database, and subshelf configuration were selected. Then click **Finish**.

Result: The shelf resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

4 **Important!** The provisioned User IDs/passwords must be used to log in to the network element.

When the reset is complete, log back into the shelf.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

END OF STEPS

Procedure 5-135.3: Clear "Subshelf Boot Failed" alarm

Steps

Complete the following steps to clear an `Subshelf Boot Failed` alarm.

1 **Important!** When the shelf is in the Maintenance Mode state, the **IND** display on the SYSCTL circuit pack faceplate shows *MPx.x* (where *x.x* is the generic number).

If the shelf is in the Maintenance Mode state, the default User IDs/passwords must be used to log in to the shelf. LUC01, LUC02, and LUC03 are the default privileged User IDs, and DMX2.5G10G is the default privileged password.

Log in to the shelf.

Result: The *Maintenance Mode Wizard (Screen 1 of 6)* appears.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

2 Perform the following to verify the generic, database, and subshelf configuration file (ssconfig.dat) on both NVMs, and reset the shelf.

1. Follow the *Maintenance Mode Wizard (Screen 1 of 6)* instructions to set the date and time and click **Next**.
2. Follow the *Maintenance Mode Wizard (Screen 2 of 6)* instructions to choose/download a generic and click **Next**.
3. Follow the *Maintenance Mode Wizard (Screen 3 of 6)* instructions to choose/download a database and click **Next**.
4. Follow the *Maintenance Mode Wizard (Screen 4 of 6)* instructions to use the selected generic and database and click **Next**.
5. Follow the *Maintenance Mode Wizard (Screen 5 of 6)* instructions to choose a subshelf configuration. and click **Next**.
6. Follow the *Maintenance Mode Wizard (Screen 6 of 6)* instructions and verify that the correct generic, database, and subshelf configuration were selected. Then click **Finish**.

   Result: The shelf resets and you are logged off the system.

   A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

3 **Important!** The provisioned User IDs/passwords must be used to log in to the shelf.

When the reset is complete, log back into the shelf.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

END OF STEPS

Procedure 5-135.4: Clear "Subshelf Configuration Mismatch" alarm

Steps

Complete the following steps to clear an `Subshelf Configuration Mismatch` alarm.

1 **Important!** The local subshelf information (subshelf MAC address and ssconfig.dat file) does not match the subshelf information provisioned on the main shelf.

Execute the **`rtrv-generic`** and **`rtrv-subshelf`** TL1 commands to obtain the local subshelf information.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) TL1 Message Details, 365-372-306*

2 Obtain office records showing the correct local subshelf information. Compare the office records with the local subshelf information obtained in Step 1.

3

If the local subshelf information is...	Then...
correct,	Perform the following: 1. Execute the **`canc-user`** TL1 command to log out of the shelf. 2. Log in to the main shelf and select **Configuration** → **Equipment** to access the subshelf information and reprovision the subshelf information correctly.
not correct,	Execute the **`ed-subshelf`** TL1 command to reprovision the local subshelf information correctly.

Result: The shelf resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) TL1 Message Details, 365-372-306*

Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

4 **Important!** The provisioned User IDs/passwords must be used to log in to the shelf.

When the reset is complete, log back into the shelf.

Reference: Procedure 6-2: “Connect Personal Computer (PC) and establish *WaveStar*® CIT session” (p. 6-27)

END OF STEPS

Procedure 5-136: Clear "SYS dorm area corrupted" condition

Overview

This procedure is used to clear a `SYS dorm area corrupted` condition.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear a `SYS dorm area corrupted` condition.

1 **Important!** The dormant generic is corrupted.

From the System View, select **Configuration** → **Software** → **Download Software** to download another dormant copy of the generic.

Reference:

- Procedure 6-16: “Ugrade software generic via SFTP” (p. 6-171)
- Procedure 6-17: “Upgrade software generic via FTP” (p. 6-175)
- Procedure 6-18: “Upgrade software generic via FTTD” (p. 6-212)
- Procedure 6-19: “Upgrade software generic via FTAM” (p. 6-218)

2 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `SYS dormant area corrupted` condition is no longer present.

END OF STEPS

Procedure 5-137: Clear "SYS generic corrupted" alarm

Overview

This procedure is used to clear a `SYS generic corrupted` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `SYS generic corrupted` alarm.

1 **Important!** The software apply operation has been interrupted/failed.

From the System View, select **Configuration** → **Software** → **Apply Software** to reschedule another *Smart* or *Smart, Override Alarms* software apply.

Result: Approximately 15 minutes after the scheduled Smart apply time, the apply is complete. You will be logged off the system when the system resets.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

Reference: Procedure 6-20: "Apply software generic" (p. 6-249)

2 Did the software apply operation complete successfully?

If...	Then...
Yes	Proceed to Step 5.
No	Continue with the next step.

3 From the System View, select **Configuration** → **Software** → **Apply Software** to schedule a Forced software apply.

Result: Approximately 15 minutes after the scheduled Forced apply time, the apply is complete. You will be logged off the system when the system resets.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

Reference: Procedure 6-20: "Apply software generic" (p. 6-249)

4 Did the Forced software apply operation complete successfully?

If...	Then...
Yes	Proceed to Step 5.
No	Contact your next level of support.

5 When the system reset is complete, log back into the network element.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar®* CIT session" (p. 6-27)

END OF STEPS

Procedure 5-138: Clear "Temporarily NUT Provisioned" condition

Overview

This procedure is used to clear a `Temporarily NUT Provisioned` condition.

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 5-7) and “Required equipment” (p. 5-7) in this chapter.
2. Refer to “Laser safety” (p. 1-6) and “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.

Steps

Complete the following steps to clear a `Temporarily NUT Provisioned` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the `Temporarily NUT Provisioned` condition in the resulting alarm list and note the corresponding AID.

2 From the System View, select **Configuration** → **Equipment**, click the **Ptn Grp** tab, highlight the 2F BLSR, and click **Select**.

Result: The *Configure Equipment* window opens.

3 In the Local NUT section of the *Configure Equipment* window, change NUT Protection Attribute to "Protected" or "Not Protected" from "Temporary not Protected", and then click **Apply**.

4 In the Provision Parameters for Equipment window, click **Close**.

5 From the System View, click the **Alarm List** button and click **Refresh**.

Result: The `Temporarily NUT Provisioned` condition is no longer present.

END OF STEPS

Procedure 5-139: Clear "Test access IP" conditions

Overview

This procedure is used to clear the following conditions:

- `Test access IP`
- `Test access IP:tsn`

Before you begin

Prior to performing this procedure, refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.

Steps

Complete the following steps to clear a `Test access IP` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button, locate the `Test access IP` condition in the resulting alarm list, and note the corresponding AID .

2 From the System View select **Fault** → **Analysis** → **Test Access** to access the *Test Access Wizard*.

3 Click **Delete an existing test access session** and **Next**.

4 Follow the directions in the remaining *Test Access Wizard* screens to delete the required test access session.

5 Verify the test access session parameters, then click **Finish** at the end of the *Test Access Wizard* screens.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes** and the *Test Access Wizard* appears. Click **Close**.

END OF STEPS

Procedure 5-140: Clear "time of day not provisioned" condition

Overview

This procedure is used to clear the `time of day not provisioned` condition.

Before you begin

Prior to performing this procedure, refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.

Steps

Complete the following steps to clear a `time of day not provisioned` condition:

1 Is the `NTP server(s) unreachable` condition in the alarm list ?

If...	Then...
Yes	Proceed to Procedure 5-104: "Clear "NTP server(s) unreachable" condition" (p. 5-266) to clear the condition. STOP! End of Procedure.
No	Continue with Step 2.

2 Using office records determine if Network Time Protocol is to be enabled at the network element.

If Network Time Protocol is...	Then...
required at the network element,	Provision Network Time Protocol as required. Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*. STOP! End of Procedure.
not required at the network element,	Proceed to Step 3.

3 From the System View, select **Administration** → **Set Date and Time**.

Result: The *Set Date and Time* window opens.

4 From the **Date** panel, select the **Year** and **Month** from the pulldown menus.

Result: A calendar is displayed for the month and year selected.

5 Click on the date from the calendar.

6 From the **Time** panel, select the **Hour**, **Minute**, and **Second** from the pulldown menus (based upon a twelve hour clock).

7 Select **am** or **pm**.

8 Click **OK**.

END OF STEPS

Procedure 5-141: Clear "Traffic Squelched" condition

Overview

This procedure is used to clear a `Traffic Squelched` condition.

Important! When this condition is present, protection switching at the BLSR node is unavailable.

Before you begin

Prior to performing this procedure, refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.

Steps

Complete the following steps to clear a `Traffic Squelched` condition.

1 Are `inc. OCN` or `inc. STSN` alarms present in the alarm list?

If...	Then...
Yes	Proceed to the appropriate procedure to clear each alarm in order of severity. Then continue with the next step.
No	Proceed to Step 4.

2 From the System View, click the **Alarm List** button and click **Refresh**.

3 Is the `Traffic Squelched` condition still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

4 **Important!** The port Application parameter of the OC-N ports that interface with the BLSR must be provisioned *2F BLSR*.

At each node in the BLSR, use **View** → **Equipment** to access the required OC-N ports and verify that the port Application parameter is provisioned *2F BLSR*.

If required, use **Configuration** → **Equipment** to access the required OC-N ports and provision the port Application parameter *2F BLSR*.

5 From the System View, click the **Alarm List** button and click **Refresh**.

6 Is the `traffic squelched` condition still present?

If...	Then...
Yes	Continue with Step 7.
No	STOP! End of Procedure.

7 From the System View, select **Reports** → **Remote NE Alarm List**.

Result: The *Remote NE Alarm List* window opens.

8 Are there alarms present on the remote NEs, especially forced switches on multiple ring nodes?

If...	Then...
Alarms	Log in to the remote NE and clear all alarms in order of severity and then continue with Step 9.
Forced Switched	Clear automatic or user-initiated ring switches until ring segmentation/isolation is eliminated and the ring is supporting a single switch request. See Procedure 5-43: “Clear "Forced Switch" condition” (p. 5-103)
No	Continue with Step 9.

9 From the System View, click the **Alarm List** button and click **Refresh**.

10 Is the `Traffic Squelched` condition still present?

If...	Then...
Yes	Continue with Step 11.
No	STOP! End of Procedure.

11 From the System View, select **View** → **Rings** → **Ring Map**. Select the required ring and click **Select**. Verify that the ring map was provisioned correctly.

Result: The *Ring Map* window opens.

12 Is either the West Link or the East Link Isolated?

If...	Then...
Yes	The adjacent node on the corresponding side (East or West) is either being initialized, powered up, powered down. What for the node to come up again and then continue with Step 13.
No	Continue with Step 13.

13 From the System View, click the **Alarm List** button and click **Refresh**.

14 Is the `Traffic Squelched` condition still present?

If...	Then...
Yes	Continue with Step 15.
No	STOP! End of Procedure.

15 Check the optical signal level and clean the cable ends if needed. If no problem is found, check the line build-outs (LBOs).

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

16 From the System View, click the **Alarm List** button and click **Refresh**.

17 Is the `Traffic Squelched` alarm still present?

If...	Then...
Yes	Continue with the next step.

If...	Then...
No	STOP! End of Procedure.

18 Are the near-end and the far-end OLIU circuit packs equipped with pluggable transmission modules?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 22.

19

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing pluggable transmission modules may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a pluggable transmission module. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the affected near-end and then the far-end pluggable transmission module.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

20 From the System View, click the **Alarm List** button and click **Refresh**.

21 Is the `Traffic Squelched` alarm still present?

If...	Then...
Yes	Remove the replacement pluggable transmission module and return the original pluggable transmission module to the socket, then continue with the next step.
No	STOP! End of Procedure.

22 **NOTICE**

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the near-end and then the far-end OLIU circuit pack.

Reference:

- Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48)
- Procedure 6-6: "Replace low-speed function unit OLIU circuit pack" (p. 6-59)

23 From the System View, click the **Alarm List** button and click **Refresh**.

If the `Traffic Squelched` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-142: Clear "unexpected CP type" alarm

Overview

This procedure is used to clear an `unexpected CP type` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `unexpected CP type` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `unexpected CP type` alarm in the resulting alarm list.

2 Determine the alarm level(s) for the active `unexpected CP type` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, and note the corresponding slot AID.

4 Using office records, determine the correct circuit pack type for the required slot.

5 Compare the correct circuit pack type from office records with the circuit pack that is physically in the required slot.

6 Is the correct circuit pack type physically installed in the required slot?

If...	Then...
Yes,	Perform the following: 1. Select **View** → **Cross-Connection**. Click the required circuit pack and **Select** to obtain a list of provisioned cross-connections for the circuit pack. 2. If required, select **Configuration** → **Cross-Connection** to access the *Cross-Connection Wizard* and delete any existing cross-connections to the circuit pack. 3. Select **Configuration** → **Update System** → **Update All**. A dialog box appears asking you to confirm executing this command. Click **Yes.**
No,	Perform the following: 1. Obtain the correct type of circuit pack (according to office records) for the required slot. 2. Replace the wrong circuit pack currently in the required slot with the correct circuit pack. Refer to the appropriate circuit pack replacement procedure in Chapter 6, “Supporting procedures”.

END OF STEPS

Procedure 5-143: Clear "unexpected or failed Pluggable Transmission Module" alarm

Overview

This procedure is used to clear an `unexpected or failed Pluggable Transmission Module` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `unexpected or failed Pluggable Transmission Module` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `unexpected or failed Pluggable Transmission Module` alarm in the resulting alarm list.

2 Determine the alarm level(s) for the active `unexpected or failed Pluggable Transmission Module` alarm(s). Clear the alarms in order of severity.

3 Refer to the Probable Cause column in the alarm list, and determine the pluggable transmission module affected and note the corresponding socket AID.

4 Was the affected pluggable transmission module just installed in the socket?

If...	Then...
Yes	Continue with Step 5.

If...	**Then...**
No	The pluggable transmission module has failed. Replace the affected pluggable transmission module. (Refer to Procedure 6-8: “Replace pluggable transmission module” (p. 6-71).) STOP! End of Procedure.

5 Use **Reports** → **Status Lists** → **Pluggable Transmission Module** to obtain the *Pluggable Transmission Module Status List* showing the expected pluggable transmission module for the affected circuit pack/socket.

6 Use the *Pluggable Transmission Module Status List* and office records to verify that the correct pluggable transmission module was installed in the correct socket/circuit pack.

If...	**Then...**
correct pluggable transmission module was installed in the *correct* socket/circuit pack,	The pluggable transmission module has failed. Replace the affected pluggable transmission module. (Refer to Procedure 6-8: “Replace pluggable transmission module” (p. 6-71).) STOP! End of Procedure.
correct pluggable transmission module was installed in the *wrong* socket/circuit pack,	Perform the following: 1. Remove the pluggable transmission module from the wrong socket/circuit pack and install the pluggable transmission module in the correct socket/circuit pack. (Refer to Procedure 6-8: “Replace pluggable transmission module” (p. 6-71).) 2. Select **Configuration** → **Update System** → **Update Inventory** to update the system equipment list. STOP! End of Procedure.

If...	Then...
wrong pluggable transmission module was installed in the *correct* socket/circuit pack,	Perform the following: 1. Replace the wrong pluggable transmission module with the correct pluggable transmission module. (Refer to Procedure 6-8: "Replace pluggable transmission module" (p. 6-71).) 2. Select **Configuration** → **Update System** → **Update Inventory** to update the system equipment list. STOP! End of Procedure.

END OF STEPS

Procedure 5-144: Clear "Unknown Ring Type" condition

Overview

This procedure is used to clear a `Unknown Ring Type` condition.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `Unknown Ring Type` condition.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button, locate the `Unknown Ring Type` condition in the resulting alarm list, and note the corresponding AID.

2 **Important!** The port Application parameter of the OC-N ports that interface with the BLSR must be provisioned *2F BLSR*.

At each node in the BLSR, use **View** → **Equipment** to access the required OC-N ports and verify that the port Application parameter is provisioned *2F BLSR*.

If required, use **Configuration** → **Equipment** to access the required OC-N ports and provision the port Application parameter *2F BLSR*.

3 From the System View, click the **Alarm List** button and click **Refresh**.

Important! While the Automatic Ring Discovery (ARD) feature updates the ring map, there will be momentary alarms, such as `Ring Prot Switching Suspended`, `Ring Discovery In Progress`. Theses will clear automatically when the ARD completes.

Result: The `Unknown Ring Type` condition is no longer present.

END OF STEPS

Procedure 5-145: Clear "unrecoverable hardware failure during download, replace CP" alarm

Overview

This procedure is used to clear an `unrecoverable hardware failure during download, replace CP` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear an `unrecoverable hardware failure during download, replace CP` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `unrecoverable hardware failure during download, replace CP` alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, and note the corresponding AID.

3 Replace the affected circuit pack.

Result: The `unrecoverable hardware failure during download, replace CP` alarm clears when the circuit pack is removed from the slot. Except for the LNW6, LNW7, and LNW16 circuit packs, the software download begins to the next circuit pack when the alarm clears. For LNW6, LNW7, and LNW16 circuit packs, the software download did not stop. When the circuit pack failed, the software download continued to the next circuit pack.

Reference: Refer to the appropriate circuit pack replacement procedure in Chapter 6, "Supporting procedures".

4 Is the affected circuit pack an LNW6 28DS1, LNW7 28DS1PM, or LNW16 12DS3EC1 circuit pack?

If ...	Then ...
Yes,	Continue with the next step.
No,	STOP! End of Procedure.

5 After the initial software download is complete, select **Configuration** → **Software** → **Apply Software** to schedule a *Smart, Override Alarms* software apply to the replacement LNW6, LNW7, or LNW16 circuit pack.

Result: Approximately 15 minutes after the scheduled apply time, the apply is complete. You will be logged off the system when the system resets.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

Reference: Procedure 6-20: "Apply software generic" (p. 6-249)

6 After the system reset is complete, log back into the shelf.

END OF STEPS

Procedure 5-146: Clear "VCG Failure of LCAS Protocol" alarms

Overview

Use this procedure to clear the following alarms:

- `VCG Failure of LCAS Protocol (Sink)`
- `VCG Failure of LCAS Protocol (Source)`

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `VCG Failure of LCAS Protocol` alarm.

1 From the System View, select **Configuration** → **Equipment**. Expand the required Ethernet circuit pack details and select the affected VCG port. Click **Select**.

2 Select the *LCAS* tab and disable the LCAS mode. Click **Apply**.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes**.

3 Re-enable the LCAS mode and click **Apply**.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes**. Click **Close** to exit window.

4 From the System View, click the **Alarm List** button and click **Refresh**.

5 Is the `VCG Failure of LCAS Protocol` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	STOP! End of Procedure.

6 Use the *WaveStar*® CIT to log in to the far-end Alcatel-Lucent 1665 DMX.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

7 At the far end, repeat Step 1 through Step 5, as required.

END OF STEPS

Procedure 5-147: Clear "VCG Loss of Partial Capacity" alarm

Overview

This procedure is used to clear a `VCG Loss of Partial Capacity` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `VCG Loss of Partial Capacity` alarm.

1 From the *WaveStar*® CIT System View, click the **Alarm List** button and locate the `VCG Loss of Partial Capacity` alarm in the resulting alarm list.

2 Are there other inc. OCN, STSN, or VT1.5 alarms in the alarm list affecting tributaries in the specified VCG?

If...	Then...
Yes	Proceed to the appropriate procedure to clear the alarm. Then continue with Step 3.
No	Continue with Step 5.

3 From the System View, click the **Alarm List** button and click **Refresh**.

4 Is the `VCG Loss of Partial Capacity` alarm still present?

If...	Then...
Yes	Continue with Step 5.
No	STOP! End of Procedure.

5 Are there `Member Signal Unacceptable-LCAS` alarms in the alarm list affecting tributaries in the specified VCG?

If...	Then...
Yes	Proceed to the appropriate procedure to clear the alarm. Then continue with Step 6.
No	Proceed to Step 8.

6 From the System View, click the **Alarm List** button and click **Refresh**.

7 Is the `VCG Loss of Partial Capacity` alarm still present?

If...	Then...
Yes	Continue with Step 8.
No	STOP! End of Procedure.

8 Are there other inc. VCG conditions/alarms in the alarm list?

If...	Then...
Yes	Proceed to the appropriate procedure to clear the alarm. Then continue with Step 9.
No	Proceed to Step 11.

9 From the System View, click the **Alarm List** button and click **Refresh**.

10 Is the `VCG Loss of Partial Capacity` alarm still present?

If...	Then...
Yes	Continue with Step 11.
No	STOP! End of Procedure.

11 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding AID.

12 From the System View, select **Fault** → **Reset** → **System Controller**.

Result: The *Reset System Controller* window opens.

13 **Important!** Do *NOT* select *Restore the system-level parameters to their default values (Phase 9)* on an in-service system. Phase 9 resets all provisionable parameters to the default values and the system controller executes a full power-up sequence.

Click *Reset the system software without changing parameters (Phase 3)*. Click **OK**.

Result: A warning appears asking you to confirm executing this command.

14 Click **Yes** to execute the command.

Result: The system resets and you are logged off the system.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

15 Log back into the network element. Click the **Alarm List** button and click **Refresh**.

16 Is the `VCG Loss of Partial Capacity` alarm still present?

If...	Then...
Yes	Continue with Step 17.
No	STOP! End of Procedure.

17

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Perform the following to remove the affected circuit pack completely from the shelf and then re-seat the circuit pack.

1. Release both circuit pack latches.
2. Remove the circuit pack from the shelf, fully disconnecting it from the backplane and removing power. The **ACTIVE** and **FAULT** LEDs extinguish.
3. Re-seat the circuit pack in the shelf.

18 From the System View, click the **Alarm List** button and click **Refresh**.

19 Is the `VCG Loss of Partial Capacity` alarm still present?

If...	Then...
Yes	Continue with Step 20.
No	STOP! End of Procedure.

20

NOTICE

Service-disruption hazard

Disconnecting cables and/or replacing circuit packs may disrupt service.

Before taking action, determine the extent of service disruption caused by disconnecting cables or replacing a circuit pack. Then, perform the action(s) deemed appropriate in light of the traffic being carried and the nature of the failure.

Replace the near-end Ethernet circuit pack.

Reference: Procedure 6-7: “Replace Ethernet/Data circuit pack” (p. 6-68)

21 From the System View, click the **Alarm List** button and click **Refresh**.

If the `VCG Loss of Partial Capacity` alarm is still present, contact your next level of support.

END OF STEPS

Procedure 5-148: Clear "version mismatch" alarm

Overview

This procedure is used to clear a `version mismatch` alarm.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 5-7) and "Required equipment" (p. 5-7) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clear a `version mismatch` alarm.

1 From the *WaveStar®* CIT System View, click the **Alarm List** button and locate the version mismatch alarm in the resulting alarm list.

2 Refer to the Probable Cause column in the alarm list, determine the affected circuit pack, and note the corresponding AID.

3 Un-seat and then re-seat the alarmed circuit pack.

Result: The SYSCTL reinitializes the affected circuit pack and should automatically update the firmware on the newly installed circuit pack.

4 From the System View, click the **Alarm List** button and click **Refresh**.

5 Is the `version mismatch` alarm still present?

If...	Then...
Yes	Continue with Step 6.
No	Proceed to Step 15.

6 From the System View, select **Configuration** → **Software** → **Apply Software** to schedule a *Smart* or *Smart, Override Alarms* software apply.

Result: Approximately 15 minutes after the scheduled apply time, the apply is complete. You will be logged off the system when the system resets.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

Reference: Procedure 6-20: "Apply software generic" (p. 6-249)

7 Log back into the shelf.

8 From the System View, click the **Alarm List** button and click **Refresh**.

9 Is the `version mismatch` alarm still present?

If...	Then...
Yes	Continue with the Step 10.
No	Proceed to Step 15.

10 From the System View, select **Configuration** → **Software** → **Apply Software** to schedule a Forced software apply.

Result: Approximately 15 minutes after the scheduled Forced apply time, the apply is complete. You will be logged off the system when the system resets.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress. During the boot, the **b** may extinguish for up to 20 seconds and then resume flashing.

Reference: Procedure 6-20: "Apply software generic" (p. 6-249)

11 Log back into the shelf.

12 From the System View, click the **Alarm List** button and click **Refresh**.

13 Is the `version mismatch` alarm still present?

If...	Then...
Yes	Continue with the next step.
No	Proceed to Step 15.

14 Un-seat and then re-seat the SYSCTL, then repeat this procedure from Step 6.

15 Are there any alarms listed?

If...	Then...
Yes	Proceed to the appropriate procedure to clear the alarm.
No	STOP! End of Procedure.

END OF STEPS

6 Supporting procedures

Overview

Purpose

This chapter contains supporting procedures for the Alcatel-Lucent 1665 Data Multiplexer.

Contents

Before you begin

Before you begin

Prior to performing *most* procedures in this ,

1. If not previously completed, install generic and *WaveStar*® CIT software on the PC. Refer to Procedure 6-1: "Install software on the PC" (p. 6-4).
2. Connect PC and establish a *WaveStar*® CIT session. Refer to Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27).

Required equipment

Most procedures in this chapter require the following equipment:

- Personal Computer (PC) with *WaveStar*® CIT software installed
- Wrist Strap

  Important! Also refer to the procedure to be performed for other equipment requirements. If other equipment is required to perform a specific procedure, that equipment is listed in the procedure.

Procedure 6-1: Install software on the PC

Overview

Use this procedure to install the *WaveStar*® CIT software and/or the NE software generic on a personal computer (PC).

Required equipment

The following equipment is required:

- Personal Computer (PC) with at least one network interface card (NIC).
- Copy of the CD-ROM that includes the *WaveStar*® CIT software and NE software.
- Current *Alcatel-Lucent 1665 Data Multiplexer (DMX) Software Release Description* for the software generic being installed.

Before you begin

Before beginning the software installation procedure, complete the following steps:

1. Become familiar with the characteristics and operating procedures of your PC and the operating system installed.
2. Ensure the user is in the administrative or power user group of the PC to install, update, modify, or repair the *WaveStar*® CIT.
3. If your PC is equipped with multiple network interface cards (NICs), know the IP address of the NIC you will be using as the *WaveStar*® CIT interface. If you are using DHCP with multiple NICs, you may need to temporarily remove all NICs except the one you plan to use for this interface.
4. Operate laptop PCs on AC power during download procedures.
5. Ensure that a laptop PC is not docked in a docking station or port replicator. Because OSI may bind to docking station NIC, you cannot install the *WaveStar*® CIT on a PC while it is in a docking station.
6. Follow proper procedures in handling the CD-ROM.
7. Read the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Software Release Description* for the software generic being installed.
8. Ensure that the list of supported network elements in the readme.txt file includes all the NEs and releases that you wish to manage with this release of the *WaveStar*® CIT.

   To access the readme.txt file, refer to the graphic in Step 2, click **Documents**, and then click **List Contents**.

Procedure

Complete the following steps to install the *WaveStar*® CIT software and/or network element software generic and on your PC.

1 With the PC *not* connected to the Alcatel-Lucent 1665 DMX shelf, insert the CD-ROM into the PC.

Result:

The CD autoruns and the following window opens:

Rxx.xx.xx in the figure represents the *WaveStar*® CIT release number, for example R24.00.00.

If the CD-ROM does not autorun, verify that the CD is inserted properly in your CD-ROM drive.

1. Double-click on My Computer on your desktop.
2. Double-click on your Compact Disc icon (often identified as drive D:).
3. Double-click on setup.exe

2 Click **continue**.

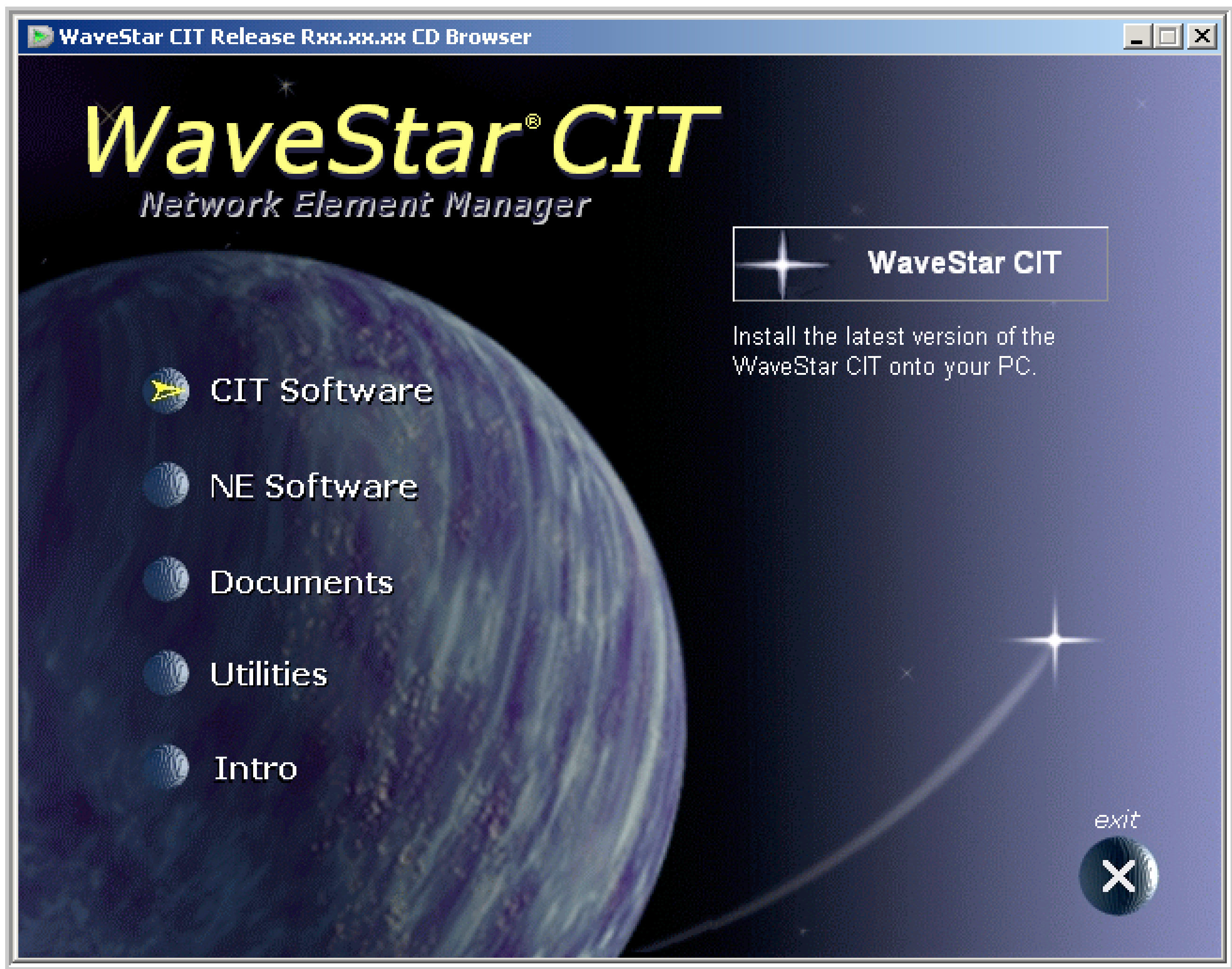
Result:

The following window opens:

3 Click **CIT Software**.

Result:

The following window appears.



4 Which software package so you wish to install on your computer?

If...	**Then...**
WaveStar® CIT software	Proceed to Procedure 6-1.1: " Install *WaveStar*® CIT software on your PC" (p. 6-9).
NE Software	Proceed to Procedure 6-20: "Apply software generic" (p. 6-249).

END OF STEPS

Procedure 6-1.1: Install *WaveStar*® CIT software on your PC

Overview

Use this procedure to install the *WaveStar*® CIT software on a personal computer (PC).

Before you begin

Before performing this procedure, complete Procedure 6-1: "Install software on the PC" (p. 6-4).

Steps

Complete the following steps to install the *WaveStar*® CIT software on your PC.

1 Click **WaveStar CIT** to install the *WaveStar*® CIT software.

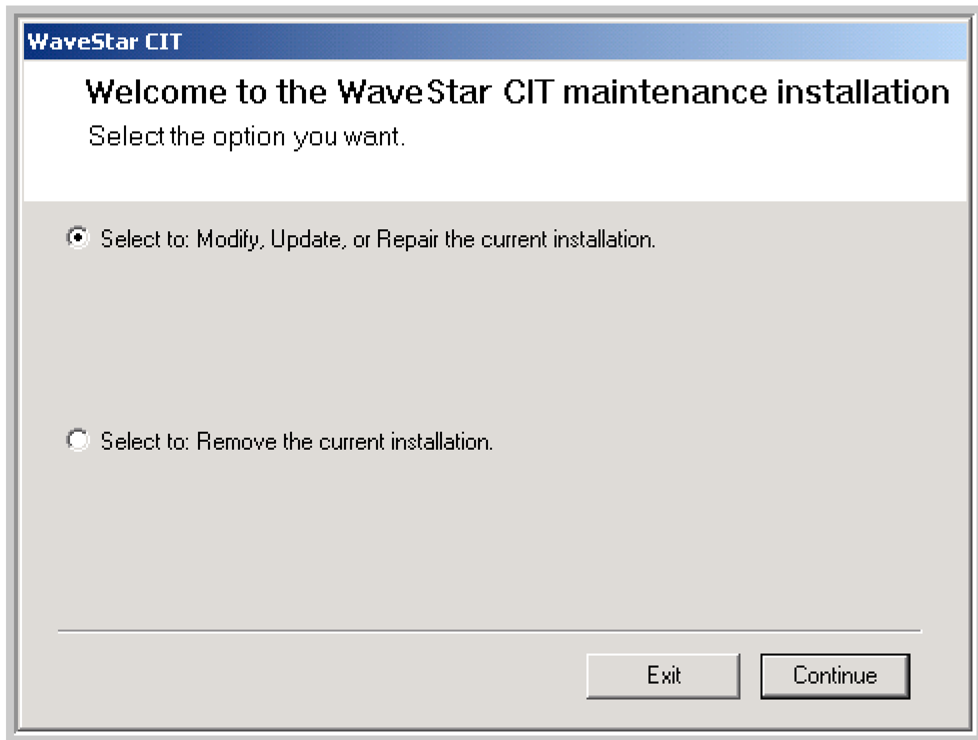
Result: Either the *WaveStar CIT InstallShield* or the *WaveStar CIT maintenance installation* screen appears.

2 A screen may appear stating that the *WaveStar*® CIT requires items (Java and/or Microsoft C++) to be installed on your computer before the installation can continue. Follow the instructions to install these items.

3 Do you have a previous version of the *WaveStar*® CIT installed on your computer?

If...	Then...
Yes	Continue with Step 4.
No	Proceed to Step 8.

4 When the following window opens, select **Select to: Modify, Update, or Repair the current installation**. Click **Continue**.



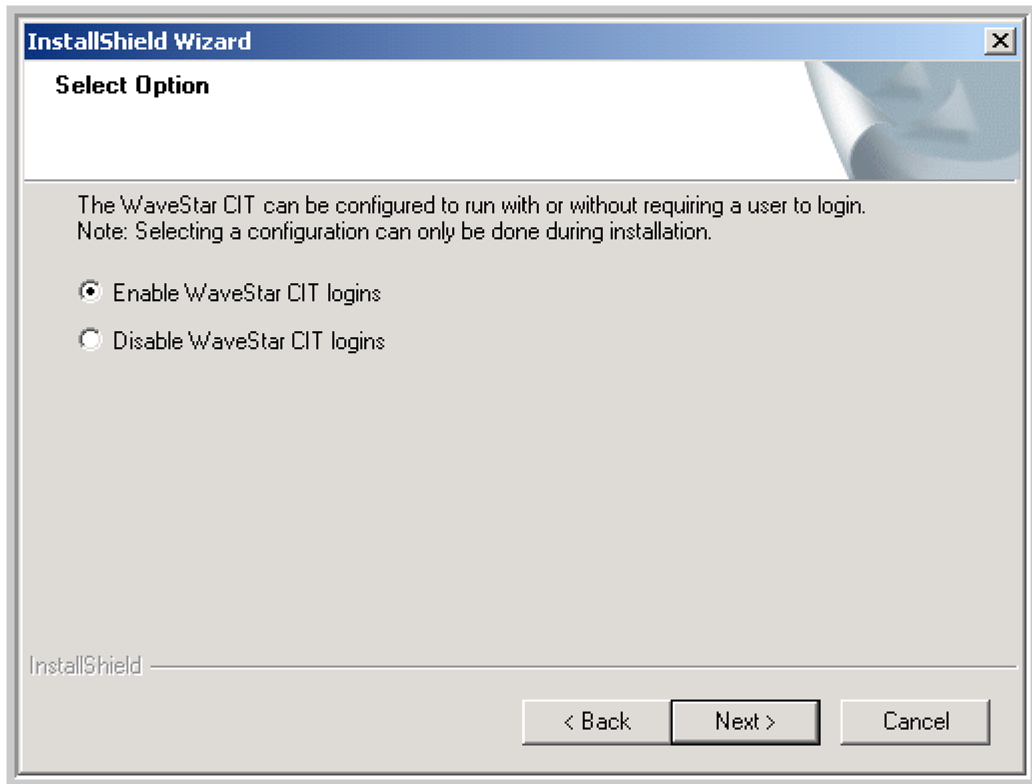
5 Select either

- **Enable WaveStar CIT logins** to require that users enter a user ID and password to login to the *WaveStar*® CIT

  or

- **Disable WaveStar CIT logins** to allow users to run the *WaveStar*® CIT without entering a user ID and password.

Click **Next**.



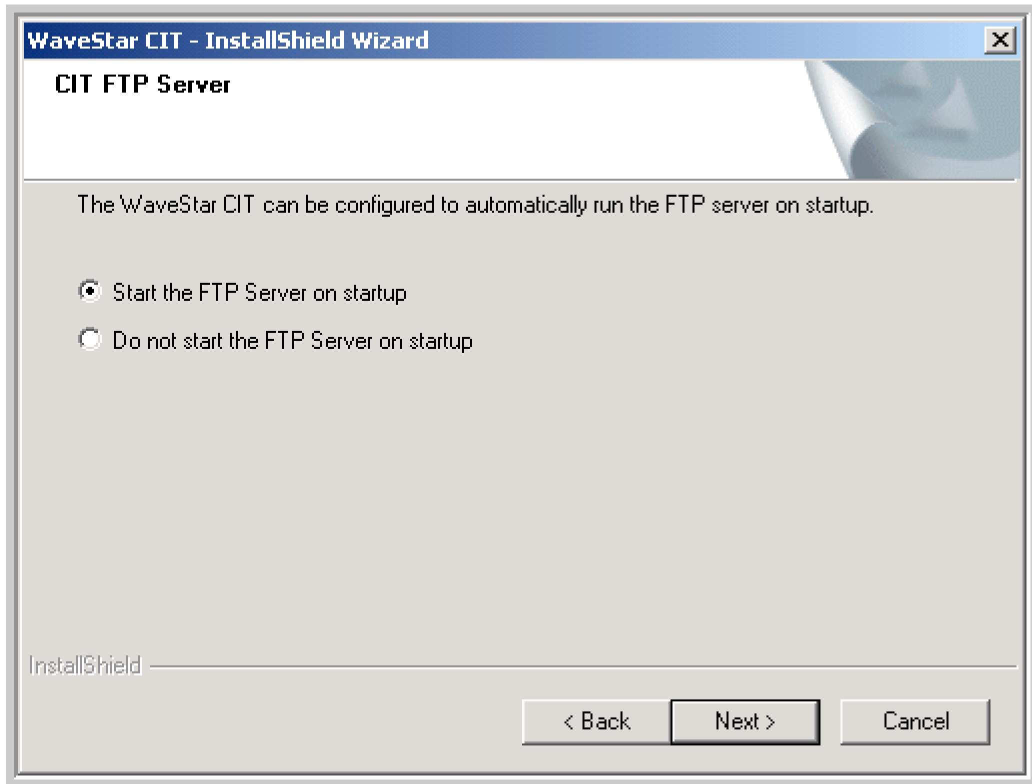
6 Select either

- **Start the FTP Server on startup**

  or

- **Do not start the FTP Server on startup**

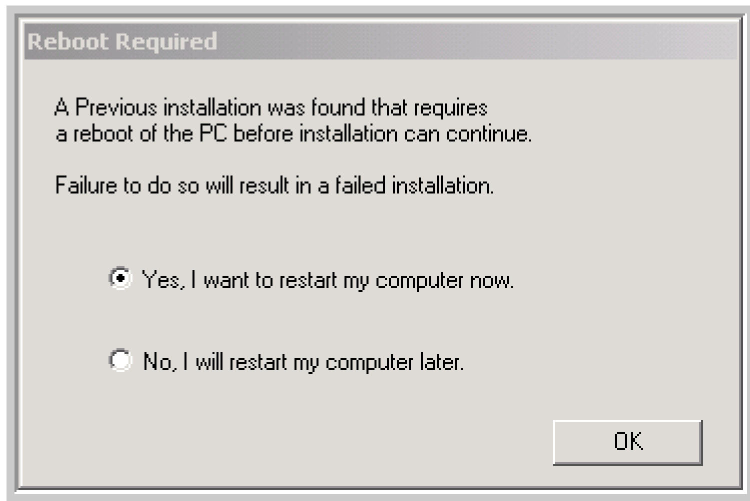
Click **Next**.



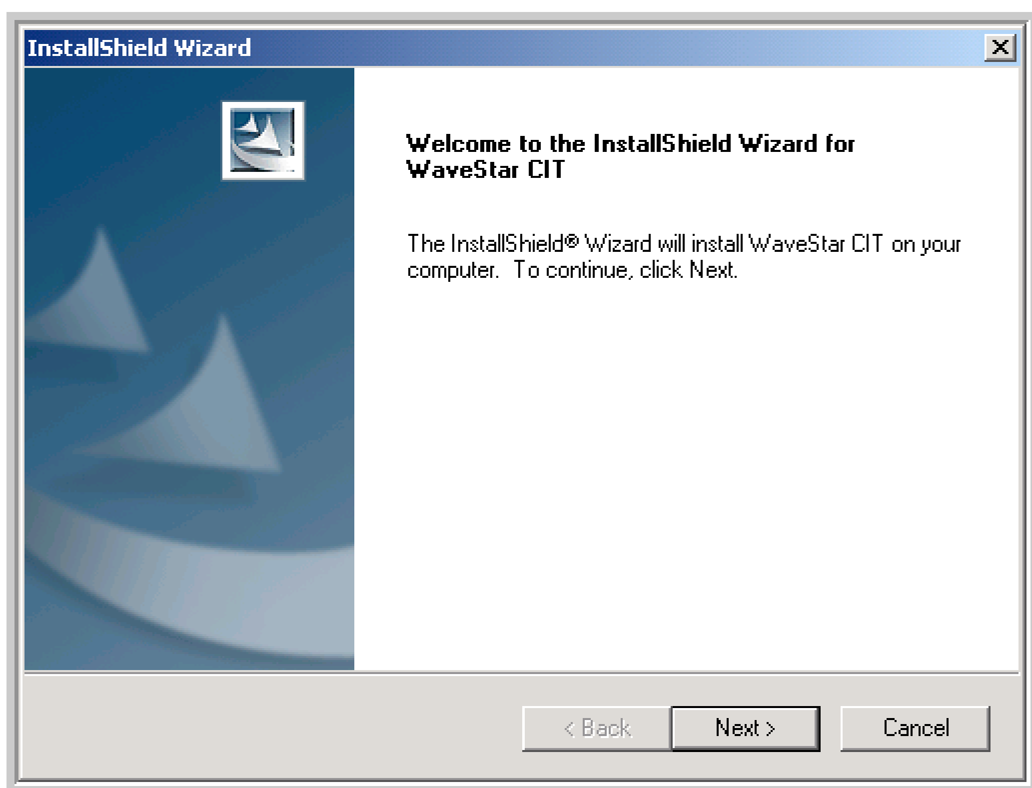
If the *WaveStar®* CIT FTP Server is not configured to automatically start on startup during installation, the FTP Server must be started manually from the Network View menu, **Administration** → **FTP Administration**.

7 Do you see the *Reboot Required* screen illustrated in this step?

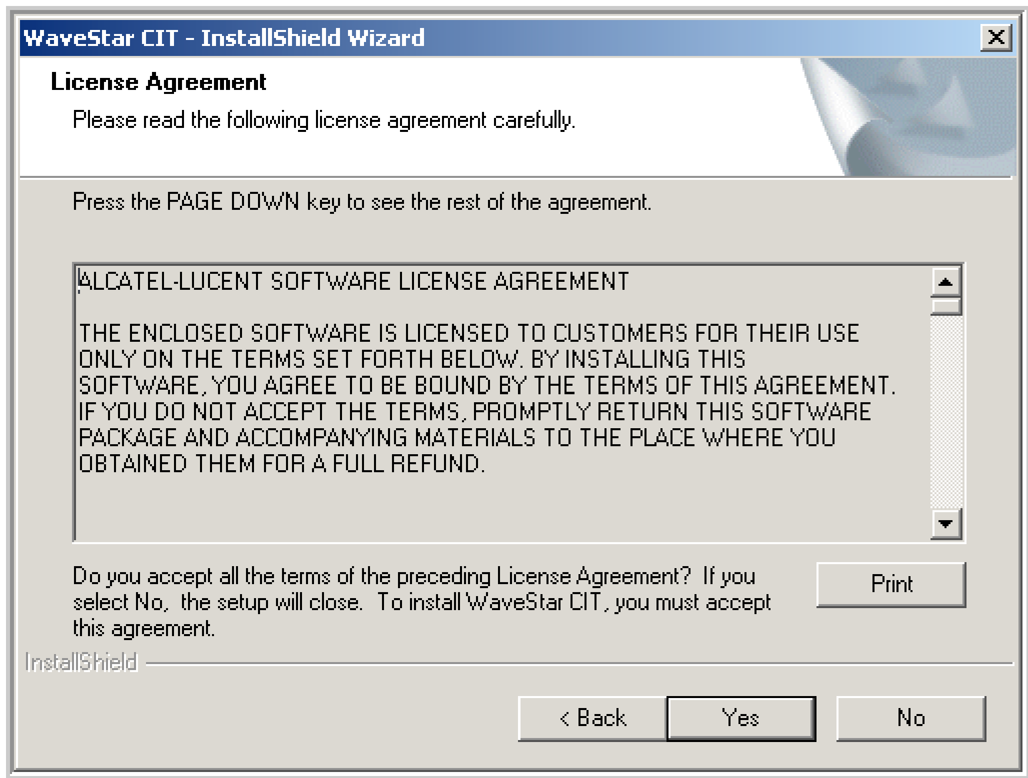
If...	Then...
Yes	The *WaveStar®* CIT installer has detected an older version of the *WaveStar®* CIT on your PC which must be removed prior to the new *WaveStar®* CIT installation. Select "**Yes, I want to restart my computer now**." Click **OK**. After your computer reboots, restart the installation from Step 1.
No	Proceed to Step 13.



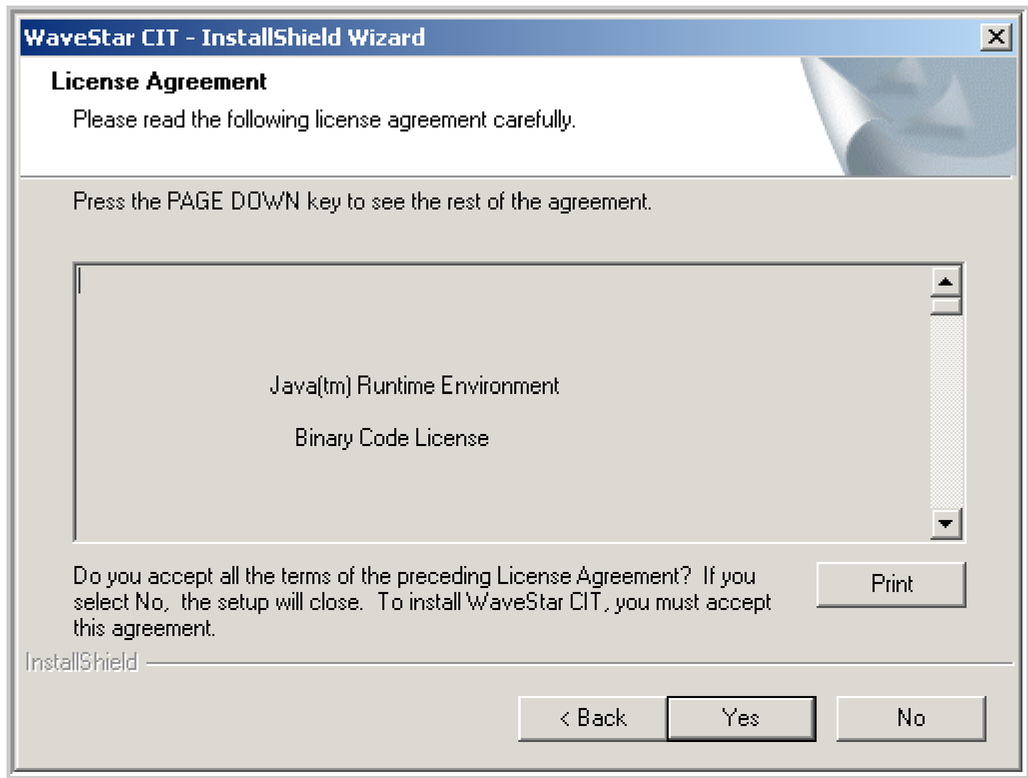
8 When the *InstallShield*® Wizard appears, click **Next**.



9 Follow the instructions on the different *InstallShield*® Wizard windows, including reading and agreeing to the following two License Agreements.



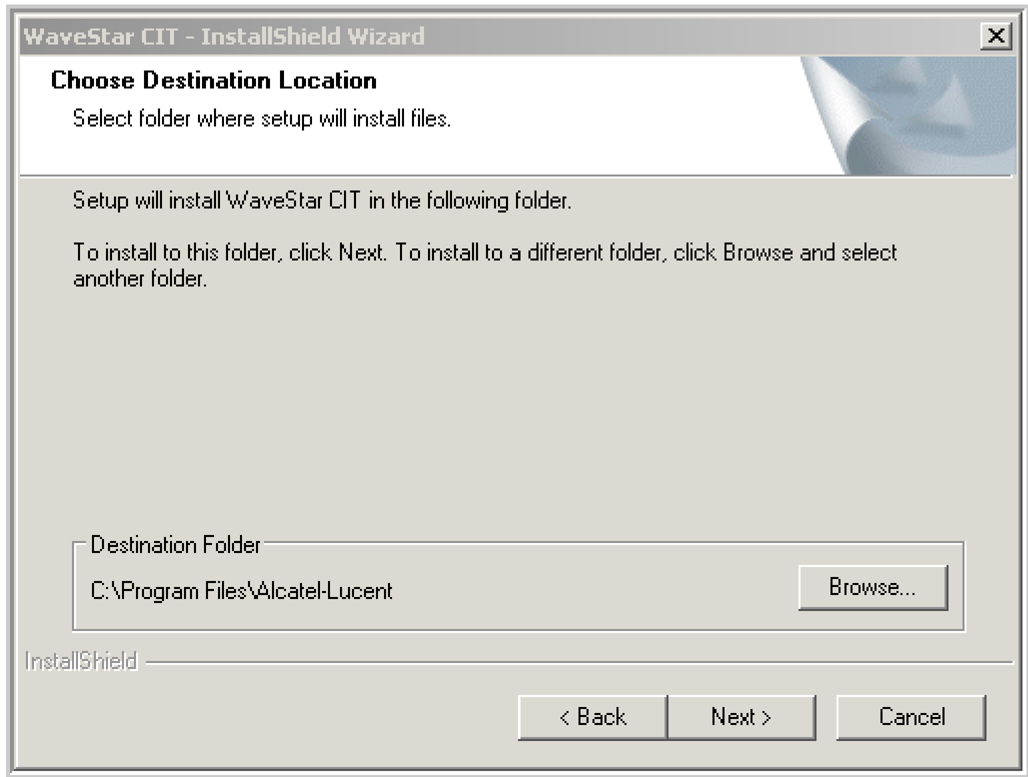
Click **Yes**.



Click **Yes**.

10 Select where you want the *WaveStar*® CIT software installed on your PC.

- Click **Next** to select the default Destination Folder: C:\Program Files\Alcatel-Lucent\. If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.
  OR
- Click **Browse** and navigate to your desired directory and then click **Next**.



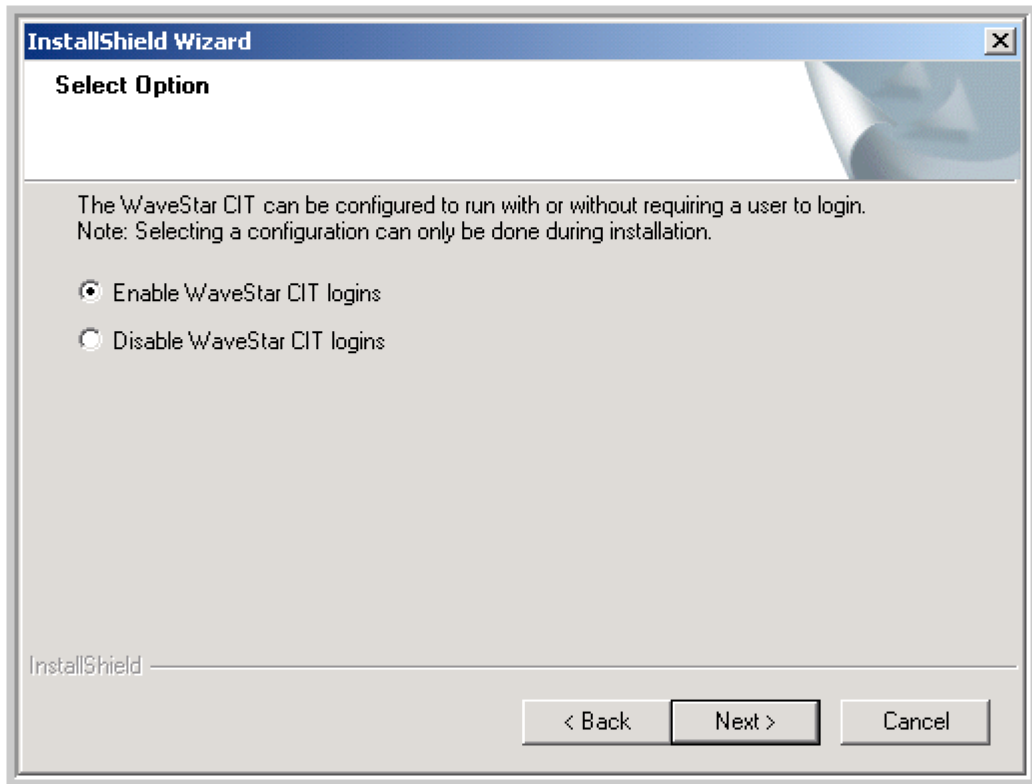
11 Select either

- **Enable WaveStar CIT logins** to require that users enter a user ID and password to login to the *WaveStar*® CIT

  or

- **Disable WaveStar CIT logins** to allow users to run the *WaveStar*® CIT without entering a user ID or password.

Click **Next**.



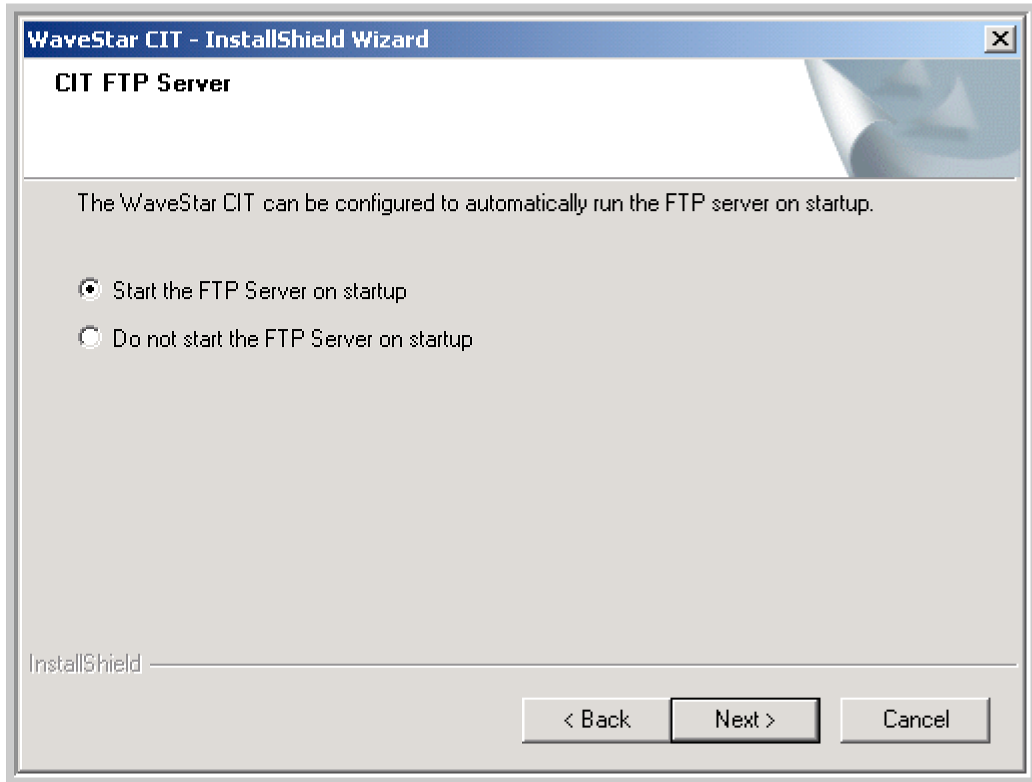
12 Select either

- **Start the FTP Server on startup**

  or

- **Do not start the FTP Server on startup**

Click **Next**.



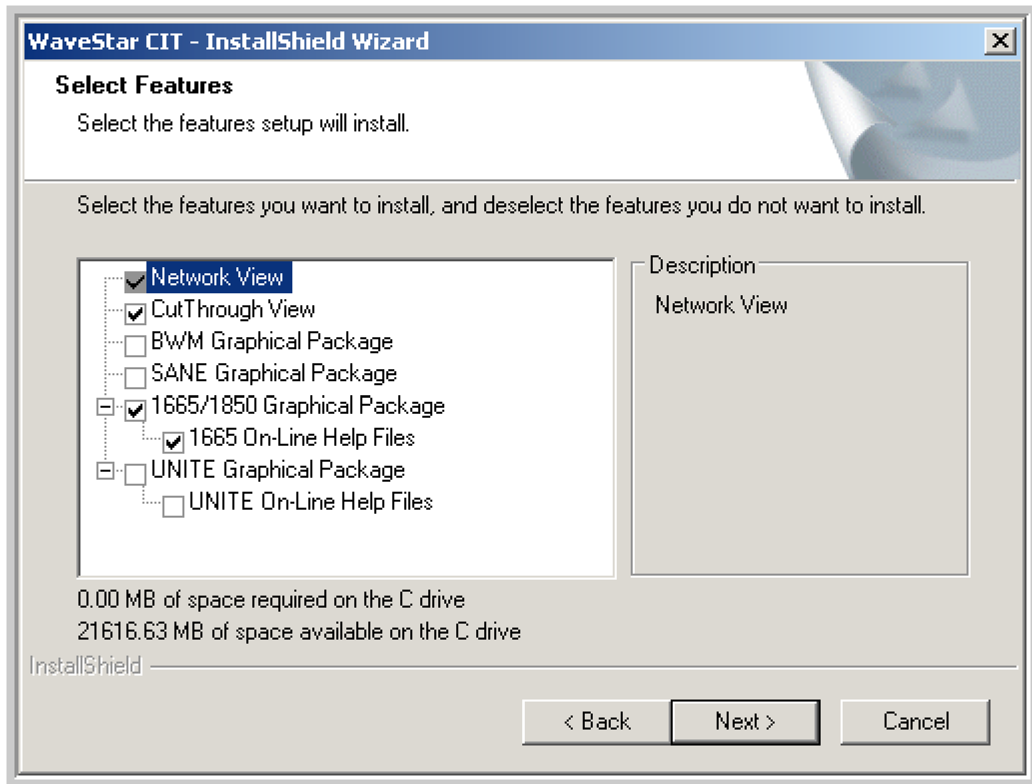
If the *WaveStar*® CIT FTP Server is not configured to automatically start on startup during installation, the FTP Server must be started manually from the Network View menu, **Administration** → **FTP Administration**.

13 Select the following components to complete the *WaveStar*® CIT installation.

- **Network View**
- **CutThrough View**
- **1665/1850 Graphical Package** installs the *WaveStar*® CIT packages for Alcatel-Lucent 1665 DMX, Alcatel-Lucent 1665 DMXtend, Alcatel-Lucent 1665 DMXplore, Alcatel-Lucent 1850 TSS-5
  - **1665 On-Line Help Files**

    If you do not wish to install online help for any of the Alcatel-Lucent 1665 products (Alcatel-Lucent 1665 DMX, Alcatel-Lucent 1665 DMXtend, Alcatel-Lucent 1665 DMXplore), you may uncheck the **1665 On-Line Help Files** box.

    Alcatel-Lucent 1850 TSS-5 does not include online help.



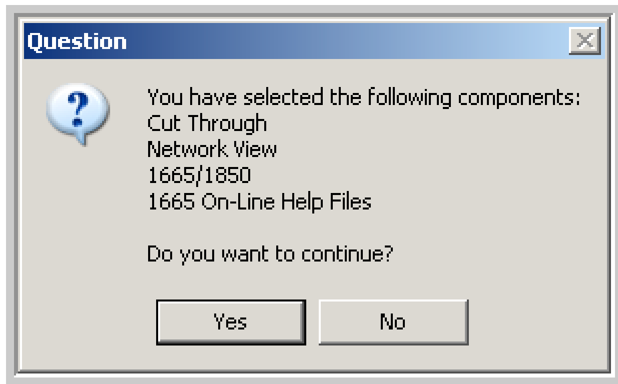
Important! The initial component selections that appear are based on the previous installation.

To save valuable disk space and reduce installation time, you can deselect graphical packages for all products that you do not plan to manage with this *WaveStar®* CIT.

Space Required on "C": indicates the space required to install you selected components. (If you specified an installation location other than Drive C, "C" may be a different drive.) If you had a previous version of the *WaveStar®* CIT installed on your computer and you are not changing your selected components, the *Space Required on "C":* is zero. In this situation, the components are already resident on the computer, therefore no additional space required when performing an upgrade. If any additional (new) packages are selected, the space required for those specific packages is displayed.

14 Click **Next**.

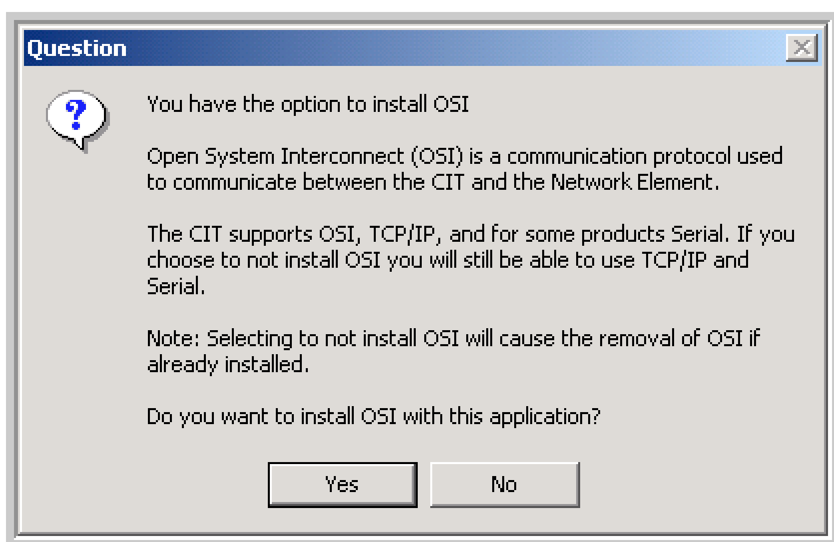
Result: The following screen appears. Confirm your component selection Your list of selected components may be different than this screen.



15 Click **Yes**.

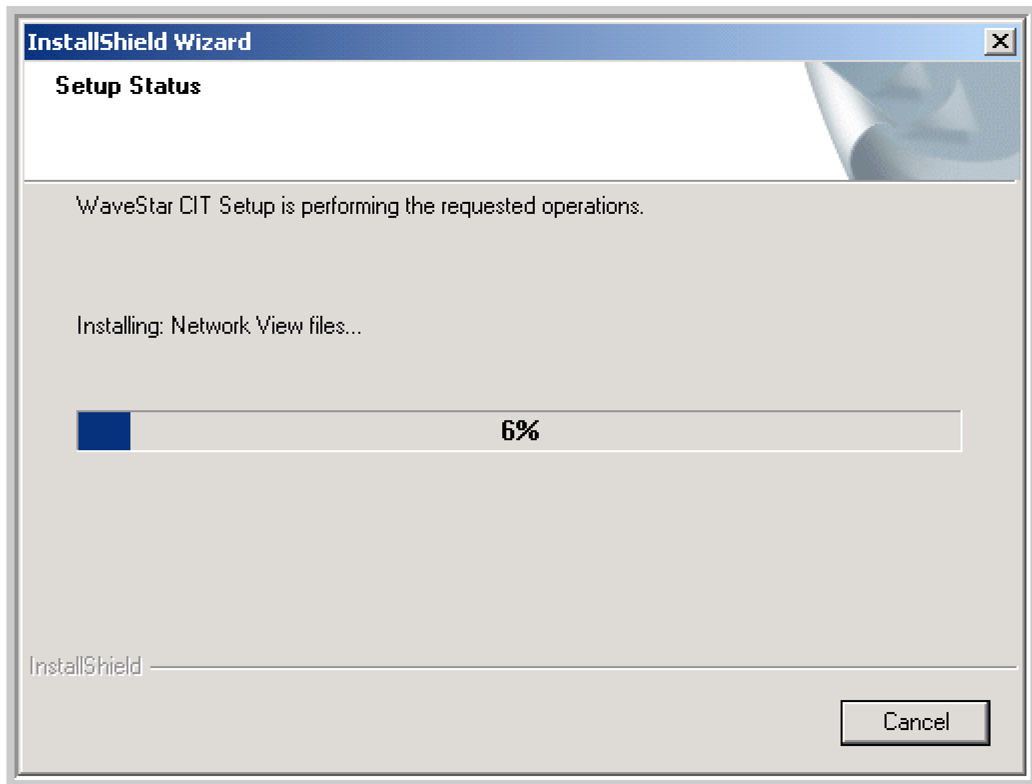
Result:

You are prompted with the choice to install OSI (Open System Interconnect) communications protocol.

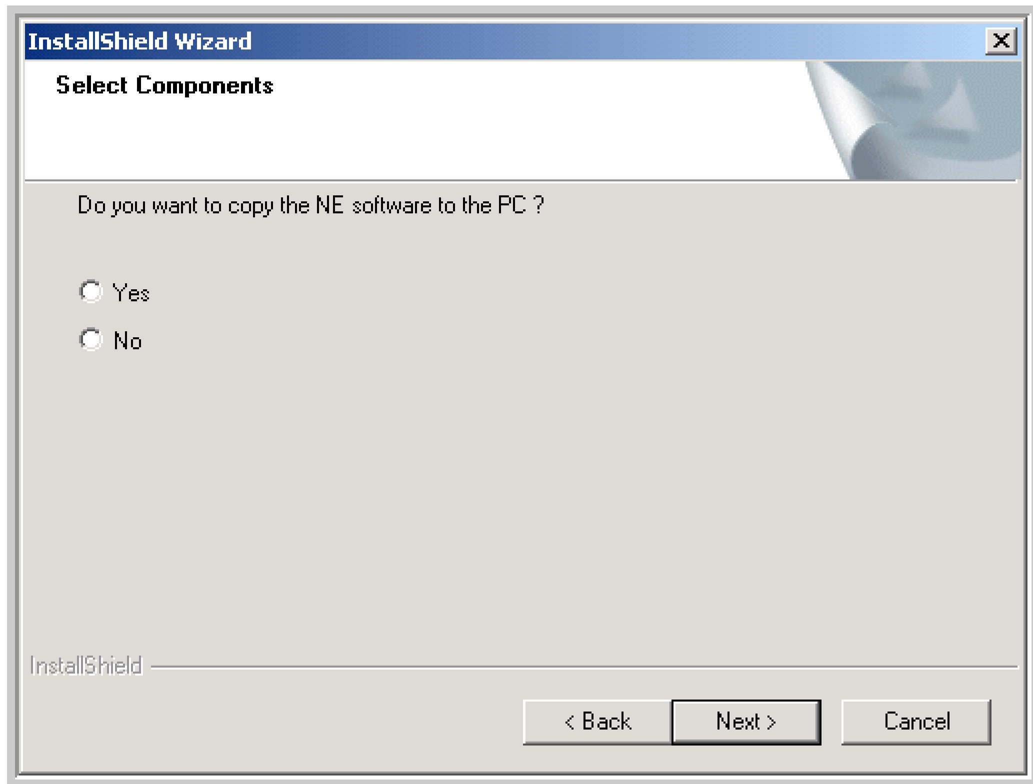


16 If you wish to install OSI click **Yes**, otherwise, click **No**.

Result: The following progress indicator screen appears while the *InstallShield*® Wizard installs the required files.



17 If you wish to copy the NE software to your PC, select **Yes** on the following screen.



18 Did you select Yes or No in Step 17?

If...	Then...
Yes	Continue with Step 19.
No	If you wish to install the NE software later, refer to Procedure 6-1.2: “Install Alcatel-Lucent 1665 DMX software on your PC” (p. 6-26). Proceed to Step 20.

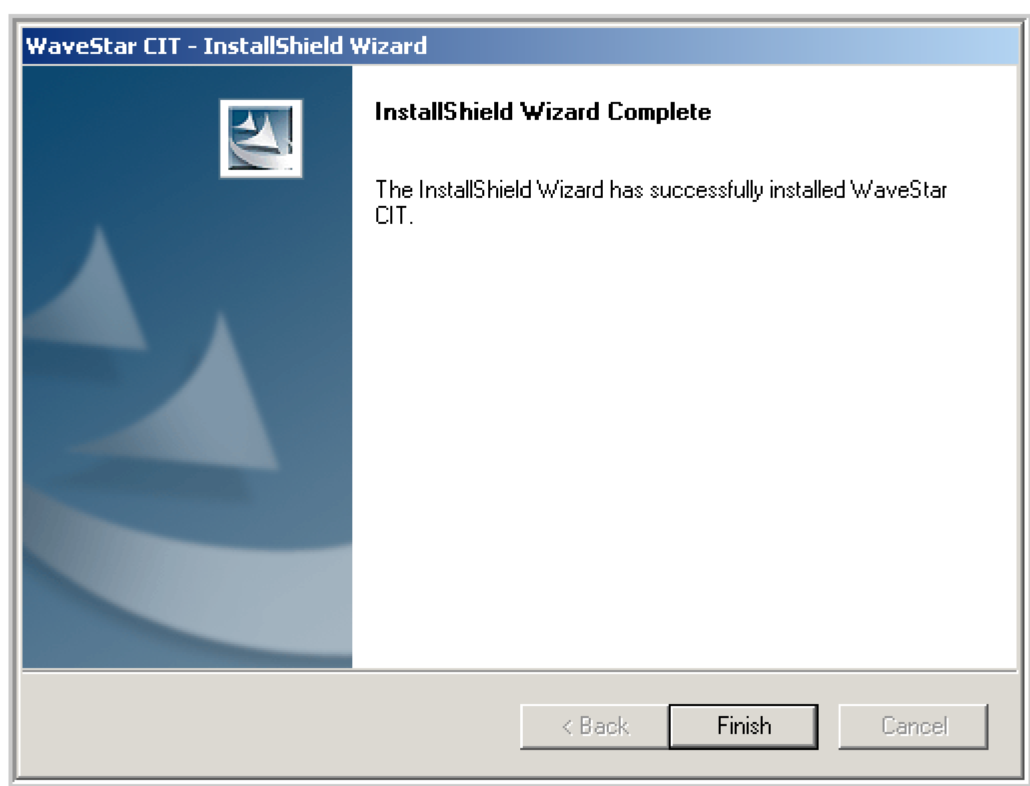
19 A *Copying files, please wait* window appears. When the window closes, the software files are successfully copied into the generics directory on your PC. By default, this directory is **`C:\Program Files\Alcatel-Lucent\WaveStar CIT\generics\DMX\9.1.x\p`**, however, the actual directory is determined by the path defined in Step 10.

Result: After the NE software is successfully copied to the appropriate directory. If you answered yes in Step 3, you may still have the following folder on your Desktop. If you answered no in Step 3, you do not see this folder.

20 In Step 16, did you elect to install OSI?

If…	Then…
No	Continue with Step 21.
Yes	Proceed to Step 24.

21 When the following screen appears, the installation without OSI is complete.

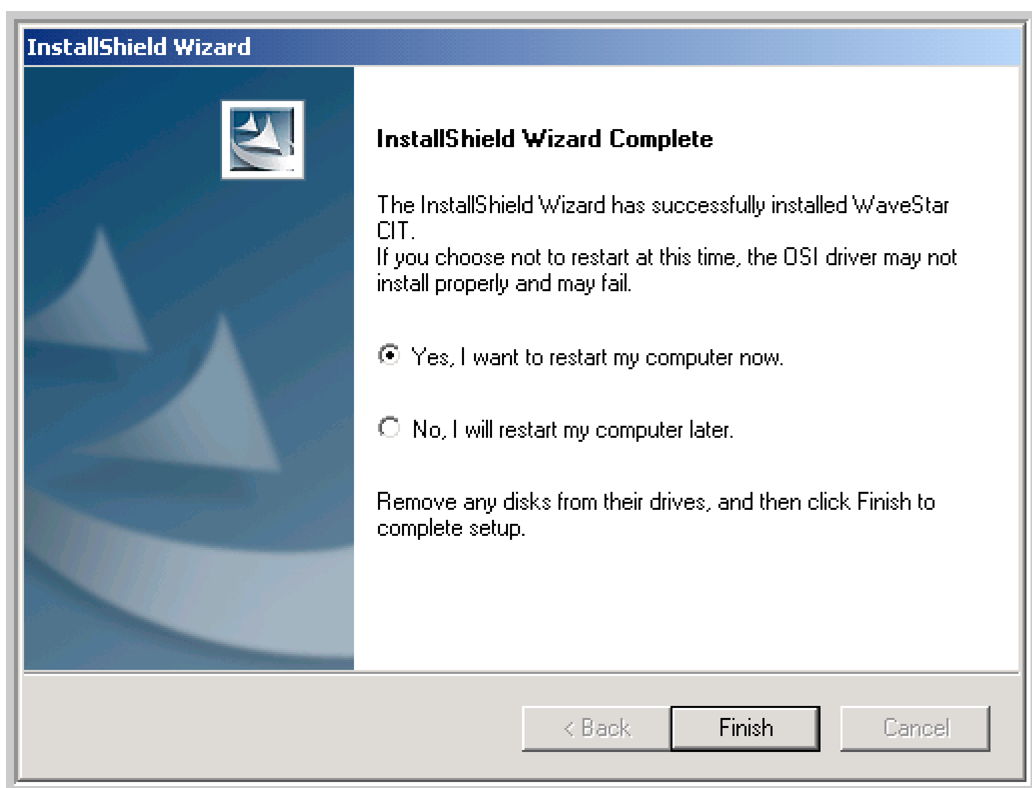


22 Click **Finish**.

Result: The following icon appears on your desktop. Click this short-cut icon to launch the *WaveStar*® CIT.

23 Proceed to Step 26.

24 When the following screen appears, the installation with OSI is complete.



25 **Important!** Before using your new *WaveStar*® CIT, you *MUST* reboot your computer.

Select **Yes, I want to restart my computer now.** and click **Finish**.

Result: The following icon appears on your desktop. After you restart your PC, click this short-cut icon to launch the *WaveStar*® CIT.

26 **Important!** The *InstallShield*® Wizard may create temporary folders/files in the PC system *Temp* folder. Temporary folders/files stored in the PC system *Temp* folder decrease available disk free space and may affect system performance.

If desired, close all open applications running on the PC and delete the appropriate temporary folders/files from the system *Temp* folder.

The *Temp* folder is defined by the TEMP system variable. It can be on any hard drive, but is usually defined as *c:\Temp*.

Windows operating systems provide a Disk Cleanup Wizard that can be used to remove temporary folders/files. To use the Disk Cleanup Wizard select **Start** → **Programs** → **Accessories** → **System Tools** → **Disk Cleanup**.

END OF STEPS

Procedure 6-1.2: Install Alcatel-Lucent 1665 DMX software on your PC

Overview

Use this procedure to install the Alcatel-Lucent 1665 DMX software on your personal computer (PC).

Before you begin

Before performing this procedure, complete Procedure 6-1: "Install software on the PC" (p. 6-4).

Steps

1 In the *WaveStar CIT CD Browser* window, click on **NE Software**, click **NE Software (Copy the NE Software to the PC)** on the right.

Result: A *Copying files, please wait* window appears.

2 When the window closes, the software files are successfully copied into the generics directory on your PC. By default, this directory is **`C:\Program Files\Alcatel-Lucent\WaveStar CIT\generics\DMX\9.1.x\p`**, however, the actual directory is determined by the path defined in Step 10 of Procedure 6-1.1: " Install *WaveStar*® CIT software on your PC" (p. 6-9).

3 Do you wish to install the *WaveStar*® CIT software?

If...	Then...
WaveStar®	Proceed to Procedure 6-1.1: " Install *WaveStar*® CIT software on your PC" (p. 6-9).
No	Stop! End of Procedure.

END OF STEPS

Procedure 6-2: Connect Personal Computer (PC) and establish *WaveStar®* CIT session

Overview

Use this procedure to connect PC and establish a *WaveStar®* CIT session.

Required equipment

At least one of the following cables is required:

- RS-232 cable with an RJ-45 connector on one end and a PC serial connector on the other (typically DB9) for the **RS232** port.
- CAT5 Ethernet straight-through or a cross-over cable for the **LAN** port. If you are connecting the PC directly to the NE, use the LAN 10Base-T cross-over cable. If you are connecting the PC directly to a hub, use the LAN 10Base-T straight-through cable.

For detailed cabling information, refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*.

Important! You must be a member of either the Administrator Group or the Power User Group on your PC to establish a *WaveStar®* CIT session.

This procedure assumes that TCP/IP and OSI connectivity has been established to the required network elements in the network.

Before you begin

Prior to performing this procedure:

1. Refer to Procedure 6-1: "Install software on the PC" (p. 6-4).
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. If *WaveStar®* CIT logins were enabled during installation, obtain a valid user ID and password for the *WaveStar®* CIT.
4. Obtain a valid user ID and password for the required network element.
5. Obtain the Target Identifier (TID)/NE name of the network element that you are establishing a *WaveStar®* CIT session with.
6. If establishing a *WaveStar®* CIT session with a network element using TCP/IP protocol, obtain the required IP address of the network element or gateway network element (if applicable).
7. If establishing a *WaveStar®* CIT session with a network element using OSI protocol, obtain the required NSAP address of the network element (if applicable). Also refer to the *CIT OSI Neighbors* view and *Address List* from the *WaveStar®* CIT Network View.

Steps

Complete the following steps to connect PC and establish a session.

1 Connect your PC (using the appropriate cable[s]) to at least one of the following ports:

- **RS232** serial port on the faceplate of the SYSCTL circuit pack to an available COM port (COM1 or COM2) of the PC
- **LAN** port on the faceplate of the SYSCTL circuit pack to the NIC card of PC. If you are connecting the PC directly to the NE, use the LAN 10Base-T cross-over cable. If you connecting the PC to a hub, use the LAN 10Base-T straight-through cable.
- **J16 IAO LAN** port on the rear of the Alcatel-Lucent 1665 DMX shelf to the NIC card of PC. If you are connecting the PC directly to the NE, use the LAN 10Base-T cross-over cable. If you are connecting the PC to a hub, use the LAN 10Base-T straight-through cable.

Important! You can be connected simultaneously to both the **RS232** and the front **LAN** or the rear **J16 IAO LAN**.

If you are uncertain that the LAN ports have already been provisioned, connecting via the serial port is recommended.

2 Start the *WaveStar*® CIT software on the PC by double-clicking on the *WaveStar*® CIT icon on your desktop (created by the installation procedure).

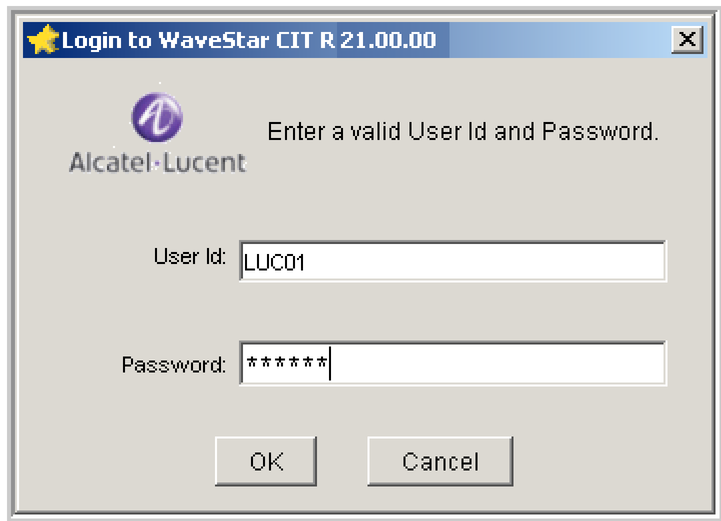
Figure 6-1 ***WaveStar*® CIT welcome window**

Rxx.xx.xx in the figure represents the *WaveStar*® CIT release number, for example R24.00.00.

3 **Important!** If you selected **Disable WaveStar CIT logins** during the *WaveStar*® CIT installation, you do not have to log in to the *WaveStar*® CIT. You will see either the Network Card selection screen (if you have more than one NIC card on your PC) or the *WaveStar*® CIT legal notice. Figure 6-3, "Legal notice" (p. 6-31).

Enter a valid User ID and password in the *WaveStar*® CIT Login window and click **OK**.

Figure 6-2 ***WaveStar*® CIT login window**

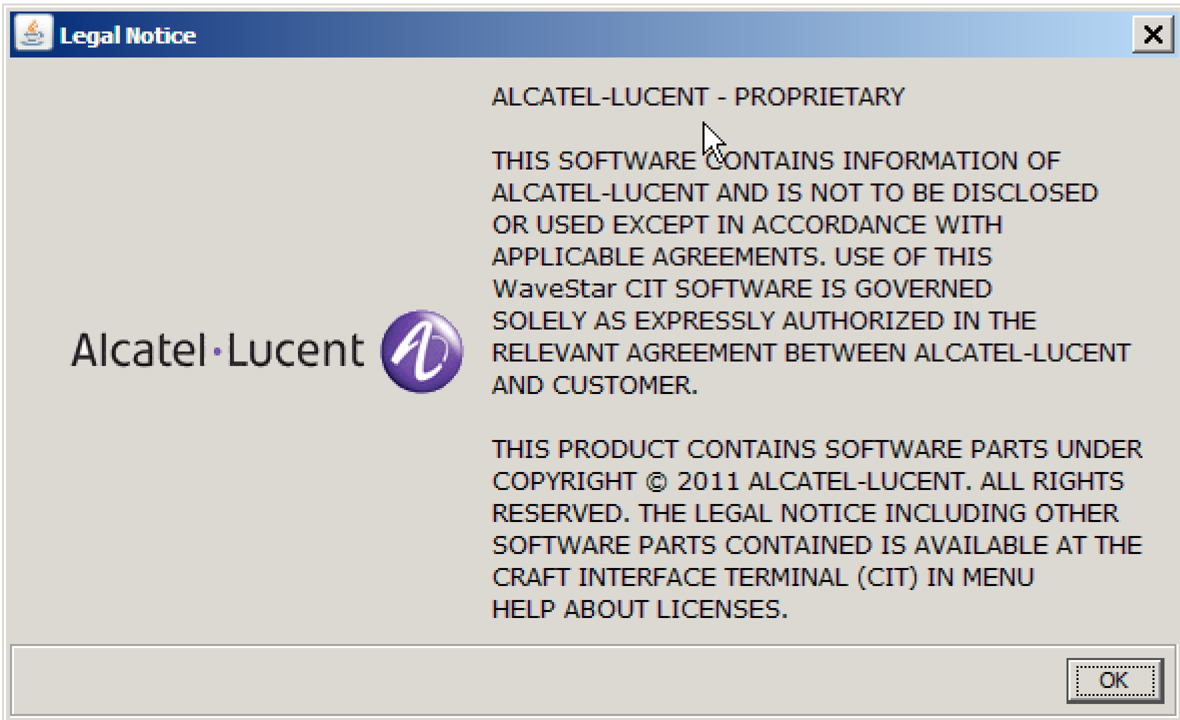


LUC01/LUC+01 and LUC02/LUC+02 are the default user IDs/passwords for the *WaveStar*® CIT. It is highly recommended that you change these user IDs and passwords during your first session to preserve the security of your equipment. To change your *WaveStar*® CIT password, select **Administration** → **Change Password** from the *WaveStar*® CIT Network View.

> **Important!** If this is the first time you are launching the *WaveStar*® CIT after a new installation or a modification, AND you have more than one Network Card on your PC, you may be asked to select the Network Card you wish to use to connect to the NE.

Result: The Legal Notice appears. (Refer to the following figure.)

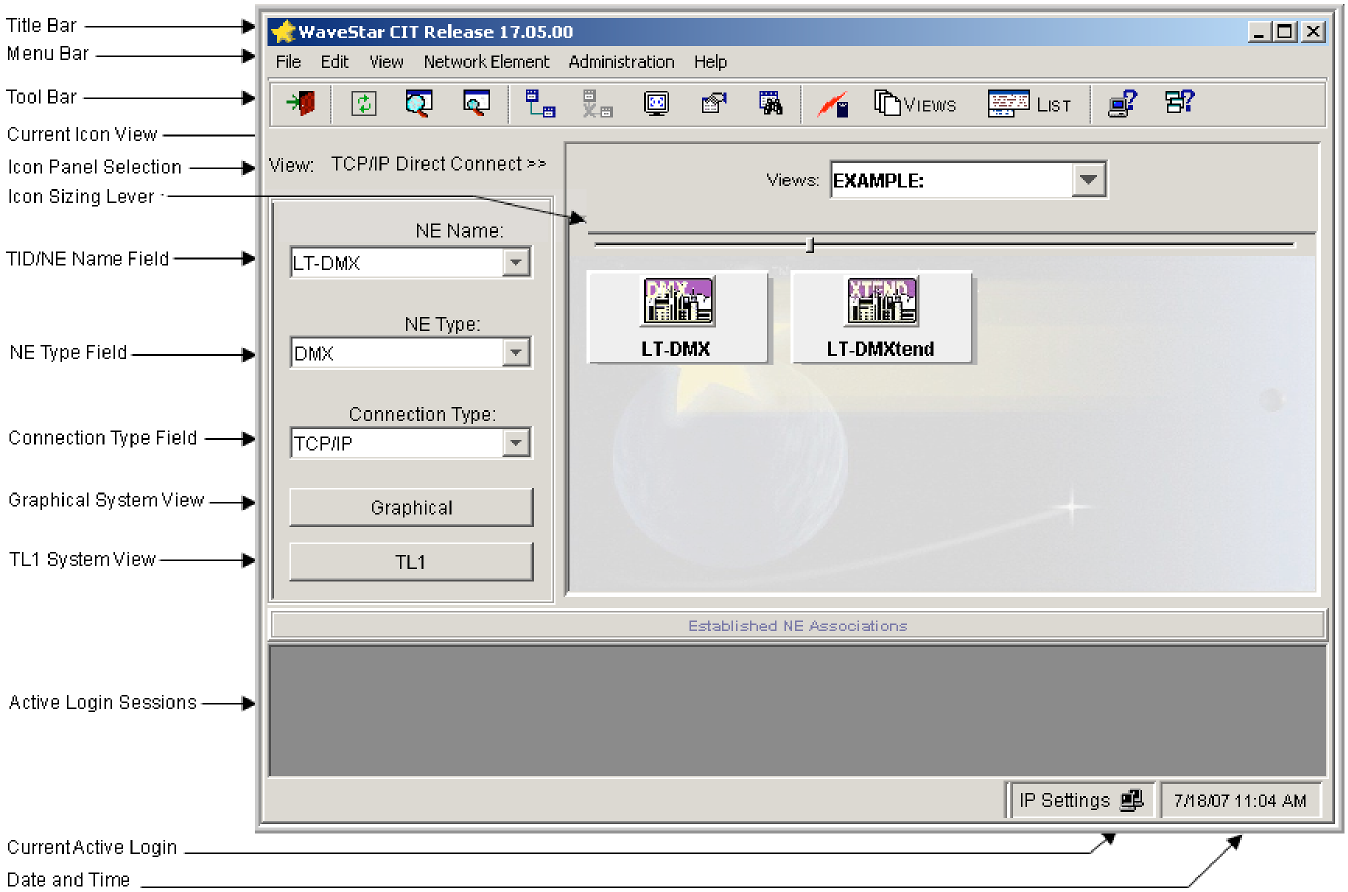
Figure 6-3 Legal notice



4 Read the Legal Notice and click **OK**.

Result: The Network View window opens. (Refer to the following figure. If your PC is running a different version of *WaveStar*® CIT software, there may be some differences between the screen shown in the following figure and what is displayed on your PC.)

Figure 6-4 Example of network view



5 Enter the NE name/TID of the shelf that you wish to communicate with in the **NE Name:** field. If you have previously established communications with the NE from this *WaveStar*® CIT, click on the drop-down arrow and select the appropriate NE from the list.

6 In the **NE Type:** field, click on the drop-down arrow and select DMX.

7 In the **Connection Type**: field, click on the drop-down arrow and select the appropriate connection type.

- *Serial* should be selected if you are connected locally to the serial **RS232** port on the SYSCTL circuit pack. To establish a *WaveStar*® CIT session to a remote network element, you must have DCC connectivity. Also refer to the *WaveStar*® CIT *CIT OSI Neighbors* view and *Address List*. See the information in "Before you begin" (p. 6-27).
- *OSI* should be selected if
  - you are connected locally to LAN-1, the front **LAN** port on the SYSCTL circuit pack, OR LAN-2, the rear **J16 IAO LAN** port on the backplane, AND
  - the LAN port is provisioned to use OSI protocol

  To establish a *WaveStar*® CIT session to a remote network element, you must have DCC connectivity. Also refer to the *WaveStar*® CIT *CIT OSI Neighbors* view and *Address List*. See the information in "Before you begin" (p. 6-27).
- *TCP/IP* should be selected if
  - you are connected locally to LAN-1, the front **LAN** port on the SYSCTL circuit pack, OR LAN-2, the rear **J16 IAO LAN** port on the backplane, AND
  - the LAN port is provisioned to use TCP/IP protocol, AND
  - you know the IP address of the NE.

  To establish a *WaveStar*® CIT session to a remote network element, you must have network connectivity and the IP address of the remote network element or gateway network element.

  Important! An IP address must be assigned to the NIC card on the PC; otherwise, login problems may occur. To assign an IP address to the NIC card, start the DOS prompt on the PC and enter the `ipconfig/all` command. An IP address line should appear. If there is no IP address line or 0.0.0.0 for an IP address, then assign an IP address to the NIC card according to local procedures.

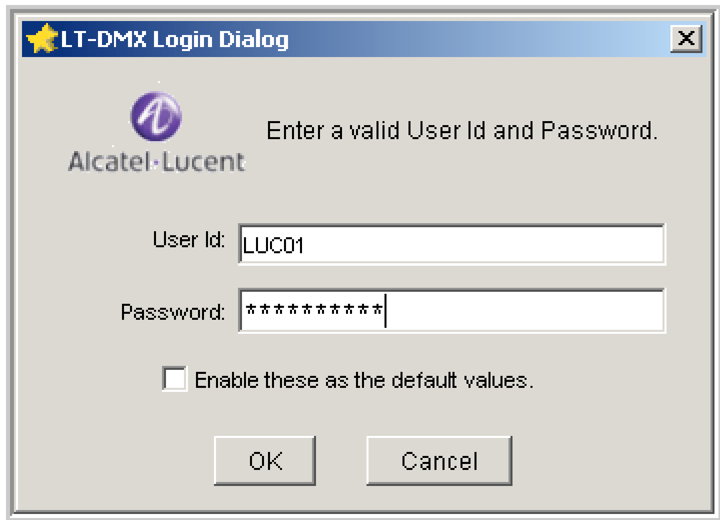
8 After completing the three fields, click on the **Graphical** button.

If you select the TCP/IP option, you must also enter the IP address of your NE and then click **OK**.

Important! All procedures in this manual assume that the Graphical button is used. However, the **TL1** button can be selected to communicate directly with the network element using the TL1 Cut Through interface.

9 An NE Login screen appears.

Figure 6-5 NE login



Enter a valid User ID and password to log in to the NE:

By selecting the **Enable these as the default values** checkbox, you will be able to reconnect to this NE without entering the User ID and Password. However, if you attempt to connect to a different NE that does not have the same User ID and password, the connection will fail and you will be prompted to enter a valid User ID and password. The User ID and Password are stored for the duration of the CIT session and must be re-entered when the CIT is restarted.

> **Important!** LUC01, LUC02, and LUC03 are the default privileged user IDs and DMX2.5G10G is the default privileged password for Alcatel-Lucent 1665 DMX. It is highly recommended that you change all three user IDs and passwords during your first session to preserve the security of your equipment.
>
> To change your network element password, refer to *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*.

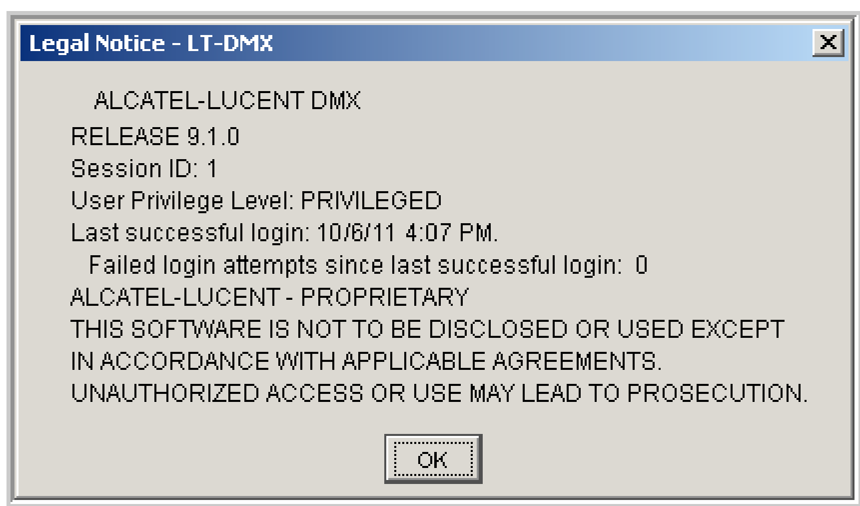
10 If the login is successful, the NE Legal Notice screen appears.

If the login is *not* successful, try one of the following:

- If you are connected locally to the **RS232** serial port, check cable connections. Check COM port baud rate settings by selecting **Administration** → **Serial COM Selection** from the *WaveStar*® CIT Network View. Try different COM port settings. The NE default baud rate setting for the **RS232** serial port (cit-1) is 9600. The rate of the COM port must match the rate of the CIT port on the NE.
- If you are connected locally to LAN-1 or LAN-2 and using the OSI protocol, check your network card (NIC) settings. Some NIC cards have an 802.1b option which must be enabled for OSI to work.
- If you are connected locally to LAN-1 or LAN-2 and using the TCP/IP protocol, make sure you are entering the correct TCP/IP address.

  Important! Your NE software Release number and User Privilege Level may be different. Your screen should be similar to Figure 6-6, “NE level legal notice” (p. 6-35).

Figure 6-6 NE level legal notice



11 Read and observe the software Release (for example, 9.1.0), and the User Privilege Level (for example, **Privileged**). Click **OK** to continue.

Important! The date and time of the last successful login and the number of unsuccessful login attempts are displayed.

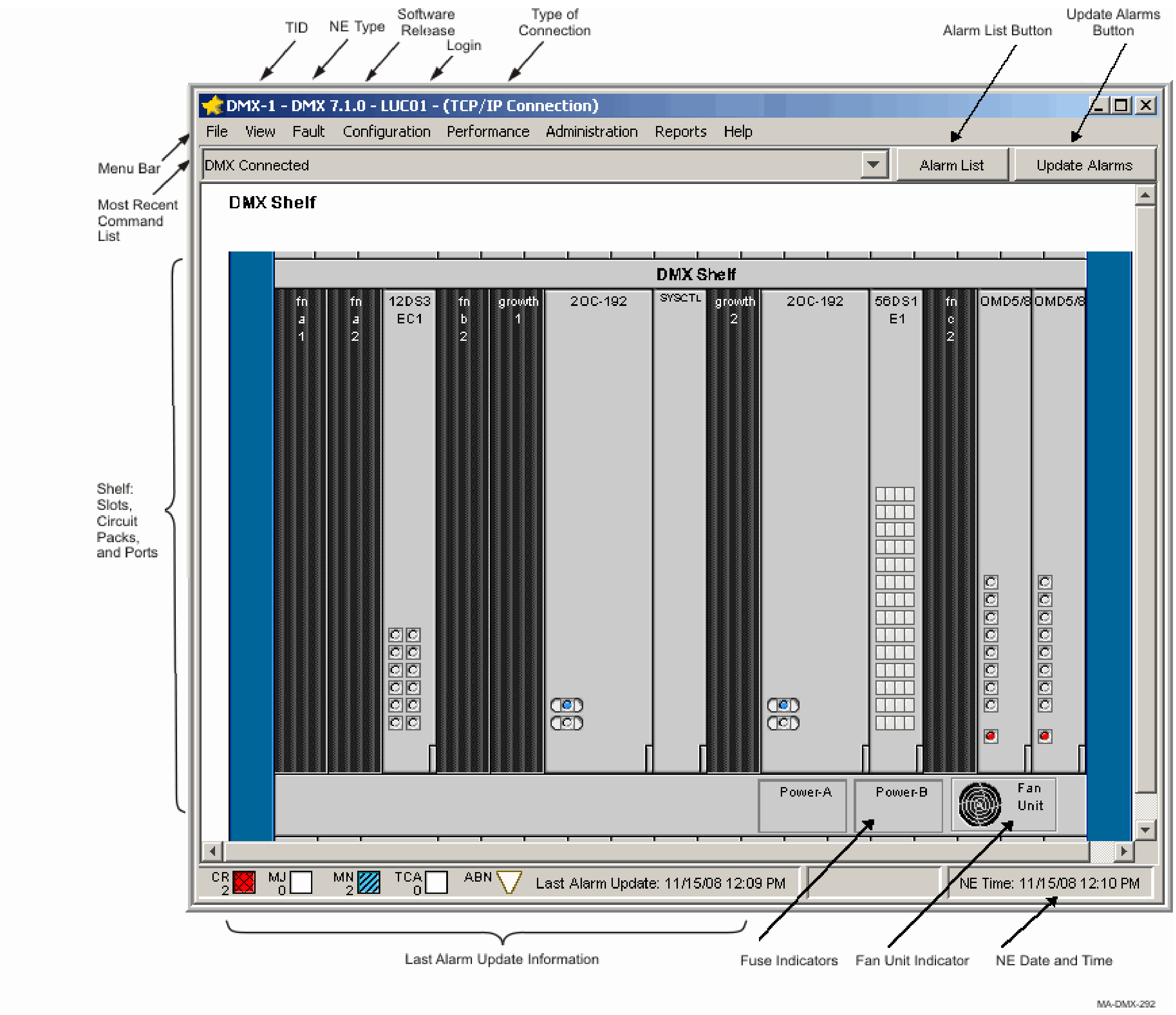
Result: The *WaveStar*® CIT System View window opens.

12 Familiarize yourself with the different aspects of the graphical presentation of the shelf, including the toolbars, and status indicators.

The *WaveStar*® CIT is designed to Microsoft *Windows*® standards.

The *WaveStar*® CIT System View has a menu bar at the top of the screen, and status indicators at the bottom of the screen. Each item on the menu bar has pull-down menus and submenus, refer to Figure 6-7, "Example of system view (graphical)" (p. 6-36).

Figure 6-7 Example of system view (graphical)



13 It is recommended that you create a View List for future convenience. From the *WaveStar*® CIT Network View window (*NOT* the System View window), select **Administration** → **Administer Views**. Click on the **Help** button and use the information on that screen to create a View List.

END OF STEPS

Procedure 6-3: Replace DS1 (LNW6/LNW7/LNW8/LNW801) circuit pack

Overview

Use this procedure to replace the following circuit packs:

- 28DS1 (LNW6)
- 28DS1PM (LNW7)
- 56DS1/E1 (LNW8)
- 56DS1/E1 (LNW801)

Important! The LNW8 and LNW801 circuit packs have common functionality and are directly interchangeable. The LNW8 and LNW801 circuit packs can occupy the same Function/Growth group together.

The system does *not* support mixing standard density (LNW6 and LNW7) in the same function group.

Important! The high-density LNW8 and LNW801 56DS1/E1 circuit packs are only compatible with the Alcatel-Lucent 1665 DMX High Capacity Shelf (DMX-HC-20A, DMX-HC-30A, or DMX-HC-30A-CE Shelf Type). The standard Alcatel-Lucent 1665 DMX Shelf does not support the high-density LNW8 and LNW801 56DS1/E1 circuit packs. If a high-density LNW8 or LNW801 56DS1/E1 circuit pack is installed in the standard Alcatel-Lucent 1665 DMX Shelf, the system will not recognize the circuit pack as an allowable type.

To determine the shelf type, select **View** → **Equipment**, highlight *Shelf*, and click **Select** to obtain the shelf details.

It is assumed that the DS1 cables have already been installed. Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304* for cabling information.

Important! If both the original circuit pack and the replacement circuit pack fail when no other transmission circuit packs are installed in the shelf, replace the SYSCTL circuit pack. Refer to Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99).

Before you begin

Prior to performing this procedure:

1. Refer to "Required equipment" (p. 6-3) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) information in Chapter 1, "Safety".
3. Ensure that the appropriate DS1 circuit pack is available for replacement.
4. Obtain work instructions for this procedure.

Steps

Complete the following steps to replace a DS1 circuit pack.

1 From the System View menu, select **View** → **Protection** to view the current protection on the circuit pack you are replacing.

2 Does 1+1 Equip appear next to the DS1 circuit pack that you wish to replace?

If...	Then...
Yes	Continue with Step 3.
No	Proceed to Step 10.

3 Highlight the Function Unit (for example: **1+1 Equip Fn-d** represents Function Unit D) containing the circuit pack you wish to replace and click **Select**.

4 Does the **Circuit Pack State** for the circuit pack that you wish to replace read **In Service**?

If...	Then...
Yes	Continue with Step 5.
No	Proceed to Step 10.

5 From the System View menu, select **Fault** → **Protection Switch**.

6 Highlight the Function Group that contains the circuit pack that you are replacing and click **Select**.

Result: On the right side of the Switch Protection window, the Switch Type: pull-down menu appears.

7 From the Switch Type: pull-down menu, select **Forced** and click **Apply**.

Result: A confirmation window appears: "Execution of provision may affect the NE service. Do you want to execute this command?"

8 On the confirmation window, click **Yes** to ensure that service switches to the other circuit pack in the Function Group. Click **Close** on the Switch Protection window.

9 To verify that the switch has occurred:

1. From the System View menu, select **View** → **Protection**.
2. Highlight the Function Group that contains the circuit pack that you are replacing and click **Select**.
3. Verify the following for the circuit pack that you are replacing:
   - Protection Switch State: reads Standby
   - Protection Switch Priority: reads Forced Switch
   - Circuit Pack State: reads Out of Service.

10 Remove the DS1 circuit pack by grasping the inner edge of the locking-levers, and applying a constant pressure, pull the levers forward and remove the circuit pack.

11 Seat the replacement DS1 circuit pack in the vacated Function Unit slot by applying steady pressure to both faceplate latches.

Result: **FAULT** LED on the DS1 circuit pack lights for approximately 20 seconds, then goes off. **ACTIVE** LED remains off. However, if your circuit pack was in-service and unprotected (refer to Step 2), then the **FAULT** LED on your replacement pack flashes until the signal is verified to be free of errors. (Firmware updates may take place that add additional wait time.)

Select **View** → **Refresh System View** and the circuit pack appears in the *WaveStar*® CIT System View indicating successful installation.

12 From the System View menu, select **Fault** → **Protection Switch**.

13 Highlight the Function Group that you force-switched and click **Select**.

Result: On the right side of the Switch Protection window, the Switch Type: pull-down menu appears.

14 From the Switch Type: pull-down menu, select **Reset** and click **Apply**.

Result: A confirmation window appears: "Execution of provision may affect the NE service. Do you want to execute this command?"

15 On the confirmation window, click **Yes** to ensure that service switches to the other circuit pack in the Function Group. Click **Close** on the Switch Protection window.

16 To verify that the forced switch is removed:

1. From the System View menu, select **View** → **Protection**.
2. Highlight the Function Group that contains the circuit pack that you replaced and click **Select**.
3. For the circuit pack that you force-switched, verify that the Protection Switch Priority: reads -.
4. For the function group, verify that the Switch Request State: reads No Request

17 Do you wish to restore the original Active/Standby states?

If...	Then...
Yes	Continue with Step 18.
No	Proceed to Step 23.

18 From the System View menu, select **Fault** → **Protection Switch**.

19 Highlight the Function Group and click **Select**.

Result: On the right side of the Switch Protection window, the Switch Type: pull-down menu appears.

20 From the Switch Type: pull-down menu, select **Manual** and click **Apply**.

Result: A confirmation window appears: "Execution of provision may affect the NE service. Do you want to execute this command?"

21 On the confirmation window, click **Yes** to ensure that service switches to the other circuit pack in the Function Group. Click **Close** on the Switch Protection window.

22 To verify that the switch has occurred:

1. From the System View menu, select **View** → **Protection**.
2. Highlight the Function Group that contains the circuit pack that you replaced and click **Select**.
3. For the circuit pack that you replaced, verify the following:
   - Protection Switch State: reads Active
   - Protection Switch Priority: reads -
   - Circuit Pack State: reads In Service.

23 From the System View menu, click the **Alarm List** button to obtain an *NE Alarm List*. Verify that no alarms are present for the installed circuit pack.

If required, refer to the appropriate procedure to clear any alarms.

24 From the System View menu, use **View** → **Equipment** to access the circuit pack/port parameters for the circuit pack just installed and verify that the parameters are intact.

If required, refer to the appropriate procedure in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* to change any circuit pack/port parameters.

END OF STEPS

Procedure 6-4: Replace DS3/EC-1/TMUX circuit pack

Overview

Use this procedure to replace the following circuit packs:

- 12DS3/EC1 (LNW16)
- TMUX (LNW18/LNW20)
- 48DS3/EC1 (LNW19/LNW19B)

Important! The high density LNW19/LNW19B 48DS3/EC1 and LNW20 TMUX circuit packs are only compatible with the Alcatel-Lucent 1665 DMX High Capacity Shelf (DMX-HC-20A, DMX-HC-30A, or DMX-HC-30A-CE Shelf Type). The standard Alcatel-Lucent 1665 DMX Shelf does not support the high density LNW19/LNW19B 48DS3/EC1 and LNW20 TMUX circuit packs. If a high density LNW19/LNW19B 48DS3/EC1 or LNW20 TMUX circuit pack is installed in the standard Alcatel-Lucent 1665 DMX Shelf, the system will not recognize the circuit pack as an allowable type.

The system does not support mixing LNW16/19/19B and LNW18/LNW20 circuit packs in the same function group.

The system does not support mixing standard density LNW16/LNW18 and high density LNW19/LNW19B/LNW20 circuit packs in the same function group.

Important! If both the original circuit pack and the replacement circuit pack fail when no other transmission circuit packs are installed in the shelf, replace the SYSCTL circuit pack. Refer to Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99).

Before you begin

Prior to performing this procedure:

1. Refer to "Required equipment" (p. 6-3) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) information in Chapter 1, "Safety".
3. Ensure that the appropriate DS3/EC-1/TMUX circuit pack is available for replacement.
4. Obtain work instructions for this procedure.

Steps

Complete the following steps to replace DS3/EC-1/TMUX circuit pack.

1 From the System View menu, select **View** → **Protection** to view the current protection on the circuit pack you are replacing.

2 Does 1+1 Equip appear next to the circuit pack that you wish to replace?

If...	Then...
Yes	Continue with Step 3.
No	Proceed to Step 10.

3 Highlight the Function Unit (for example: **1+1 Equip Fn-d** represents Function Unit D) that contains the circuit pack that you are replacing and click **Select**.

4 Does the **Circuit Pack State** for the circuit pack that you wish to replace read **In Service**?

If...	Then...
Yes	Continue with Step 5.
No	Proceed to Step 10.

5 From the System View menu, select **Fault** → **Protection Switch**.

6 Highlight the Function Group that contains the circuit pack that you are replacing and click **Select**.

Result: On the right side of the Switch Protection window, the Switch Type: pull-down menu appears.

7 From the Switch Type: pull-down menu, select **Forced** and click **Apply**.

Result: A confirmation window appears: "Execution of provision may affect the NE service. Do you want to execute this command?"

8 On the confirmation window, click **Yes** to ensure that service switches to the other circuit pack in the Function Group. Click **Close** on the Switch Protection window.

9 To verify that the switch has occurred:

1. From the System View menu, select **View** → **Protection**.
2. Highlight the Function Group that contains the circuit pack that you are replacing and click **Select**.
3. Verify the following for the circuit pack that you are replacing:
   - Protection Switch State: reads Standby
   - Protection Switch Priority: reads Forced Switch
   - Circuit Pack State: reads Out of Service.

10 Remove the circuit pack by grasping the inner edge of the locking-levers, and applying a constant pressure, pull the levers forward and remove the circuit pack.

11 Seat the replacement circuit pack in the vacated Function Unit slot by applying steady pressure to both faceplate latches.

Result: **FAULT** LED on the circuit pack lights for approximately 20 seconds, then goes off. **ACTIVE** LED remains off. However, if your circuit pack was in-service and unprotected (refer to Step 2), then the **FAULT** LED on your replacement pack flashes until the signal is verified to be free of errors. (Firmware updates may take place that add additional wait time.)

Select **View** → **Refresh System View** and the circuit pack appears in the *WaveStar*® CIT System View indicating successful installation.

12 From the System View menu, click the **Alarm List** button to obtain an *NE Alarm List*. Verify that no alarms are present for the installed circuit pack.

If required, refer to the appropriate procedure to clear any alarms.

13 Do you wish to restore the original Active/Standby states?

If ...	Then...
releasing a forced switch is required,	Continue with the next step.
releasing a forced switch is *not* required,	Proceed to Step 26.

14 From the System View menu, select **Fault** → **Protection Switch**.

15 Highlight the Function Group that you force-switched and click **Select**.

Result: On the right side of the Switch Protection window, the Switch Type: pull-down menu appears.

16 From the Switch Type: pull-down menu, select **Reset** and click **Apply**.

Result: A confirmation window appears: "Execution of provision may affect the NE service. Do you want to execute this command?"

17 On the confirmation window, click **Yes** to ensure that forced switch is released. Click **Close** on the Switch Protection window.

18 To verify that the forced switch is removed:

1. From the System View menu, select **View** → **Protection**.
2. Highlight the Function Group that contains the circuit pack that you replaced and click **Select**.
3. For the circuit pack that you force-switched, verify that the Protection Switch Priority: reads -.
4. For the function group, verify that the Switch Request State: reads No Request

19 Do you wish to restore the original Active/Standby states?

If...	Then...
Yes	Continue with Step 20.
No	Proceed to Step 25.

20 From the System View menu, select **Fault** → **Protection Switch**.

21 Highlight the Function Group and click **Select**.

Result: On the right side of the Switch Protection window, the Switch Type: pull-down menu appears.

22 From the Switch Type: pull-down menu, select **Manual** and click **Apply**.

Result: A confirmation window appears: "Execution of provision may affect the NE service. Do you want to execute this command?"

23 On the confirmation window, click **Yes** to ensure that service switches to the other circuit pack in the Function Group. Click **Close** on the Switch Protection window.

24 To verify that the switch has occurred:

1. From the System View menu, select **View** → **Protection**.
2. Highlight the Function Group that contains the circuit pack that you replaced and click **Select**.
3. For the circuit pack that you replaced, verify the following:
   - Protection Switch State: reads Active
   - Protection Switch Priority: reads -
   - Circuit Pack State: reads In Service.

25 From the System View menu, click the **Alarm List** button to obtain an *NE Alarm List*. Verify that no alarms are present for the installed circuit pack.

If required, refer to the appropriate procedure to clear any alarms.

26 From the System View menu, use **View** → **Equipment** to access the circuit pack/port parameters for the circuit pack just installed and verify that the parameters are intact.

If required, refer to the appropriate procedure in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* to change any circuit pack/port parameters.

END OF STEPS

Procedure 6-5: Replace high-speed main OLIU circuit pack

Overview

Use this procedure to replace a high-speed OC-12/OC-48/OC-192 OLIU circuit pack that is installed in a main slot (M1 or M2).

Important! The OLIU circuit packs in the Main slots *must* both have the same optical line rate and VT cross-connect size. If the circuit packs in the Main slots have different optical line rates or VT cross-connect sizes, the system reports an `unexpected CP type` alarm and service may be impacted.

Important! If responses are not correct when replacing the main OLIU circuit pack, check the connections. If the connections are correct, replace the circuit pack with the wrong response. (The red FAULT LED normally flashes when an OLIU circuit pack is monitored and there is no signal present.)

If both the original OLIU circuit pack and the replacement OLIU circuit pack fail when no other transmission circuit packs are installed in the shelf, replace the SYSCTL circuit pack. Refer to Procedure 6-10: “Upgrade or replace SYSCTL (LNW2) circuit pack” (p. 6-99).

Required equipment

In addition to the equipment listed in “Required equipment” (p. 6-3), the following equipment is also required:

- Erasable marker or pencil
- Optical loopback cables, LBOs, and optical fiber cleaning tools (if loopbacks are performed)

Use only Alcatel-Lucent Approved Class 1 SFP/XFP transceivers. Refer to the list of pluggable transmission modules in Procedure 6-8: “Replace pluggable transmission module” (p. 6-71).

Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*, as required, when removing and/or installing pluggable transmission modules.

Before you begin

Prior to performing this procedure:

1. Refer to “Laser safety” (p. 1-6) and “Electrostatic discharge” (p. 1-26) information in Chapter 1, “Safety”.
2. Obtain the work instructions for this procedure. It is especially important to know desired wavelengths and enhanced mode requirements (12 STS-1s) when applicable.

3. If required, ensure that the correct pluggable transmission modules are available for replacement.
4. Ensure that correct OC-12/48/192 OLIU circuit packs are available for installation.

   The OLIU circuit packs in Main slots *must* have the same size VT cross-connect fabric. For example, the LNW27 and LNW29 OC-48 OLIU circuit packs have full (up to 48 STS-1s) VT mapping; therefore, they can be used together in the Main slots. If the circuit packs in the Main slots have different VT cross-connect fabric sizes, the system reports an `unexpected CP type` alarm.

   The following is a list of Main OLIU circuit packs grouped by switch fabric:

   - OC-12 OLIUs with 12 STS-1 switch fabric: LNW48 LNW50 LNW54 LNW203
   - OC-48 OLIUs with 12 STS-1 switch fabric: LNW26B (jumper set to enhanced) LNW28 (jumper set to enhanced) LNW77 (jumper set to enhanced) LNW121B—LNW159B (jumper set to enhanced)

     LNW26B, LNW28, LNW77, LNW121B—LNW159B OC-48 OLIUs with 6 STS-1 switch fabric (jumper set to normal) are not supported in Release 6.0.

     The LNW26B, LNW28, LNW77, and LNW121B-159B OLIU circuit packs are DA'ed and are no longer available.
   - OC-48 OLIUs with 48 STS-1 switch fabric: LNW27 LNW29 LNW32 LNW76 LNW202 LNW221—LNW259
   - OC-192 OLIUs with 48 STS-1 switch fabric: LNW56 LNW57 LNW58 LNW60 LNW502 LNW523 LNW527 LNW554 LNW555
   - Very Large Fabric OC-192 OLIUs with 192 STS-1 switch fabric: LNW59
   - Very Large Fabric multirate OC-3/12/48 OLIUs with 192 STS-1 switch fabric: LNW82
   - Very Large Fabric multirate OC-48/192 OLIUs with 192 STS-1 switch fabric: LNW504

   Important! The Very Large Fabric LNW59 and LNW82 circuit packs are only compatible with the Alcatel-Lucent 1665 DMX High Capacity Shelf (DMX-HC-20A, DMX-HC-30A, or DMX-HC-30A-CE Shelf Type). The Standard Alcatel-Lucent 1665 DMX Shelf does not support LNW59 and LNW82 circuit packs. If LNW59 and LNW82 circuit packs are installed in the Standard Alcatel-Lucent 1665 DMX Shelf, the system will not recognize the circuit pack as an allowable type.

   To determine the shelf type, select **View** → **Equipment**, highlight *Shelf*, and click **Select** to obtain the shelf details.

Steps

Complete the following steps to replace an OLIU circuit pack in M1 or M2.

1 From the System View menu, select **View** → **Timing/Sync** and select the System Timing tab. The Active Circuit Pack item reads either main-1 or main-2.

2 Is the OLIU circuit pack that you wish to replace the active circuit pack?

If...	**Then...**
Yes	Continue with Step 3.
No	Proceed to Step 7.

3 Is the Alcatel-Lucent 1665 DMX shelf line timed from the main OLIU that you are replacing?

If...	**Then...**
Yes	Continue with Step 4.
No	Proceed to Step 7.

4 From the System View menu, select **View** → **Timing/Sync** and click the **System Timing** tab.

5 Is system autoreconfiguration enabled?

If...	**Then...**
Yes	Proceed to Step 7.
No	Continue with Step 6.

6 From the System View menu, select **Configuration** → **Timing/Sync** and click the **System Timing** tab. Select Enable in the Synchronization Autoreconfiguration field. Click **OK**.

Important! Enable synchronization autoreconfiguration before removing the active circuit pack to ensure synchronization reference protection switching. If synchronization autoreconfiguration is disabled, and the active circuit pack is removed, the system enters holdover.

7 Prepare to remove the circuit pack:

1. Grasp the inner edges of the locking levers that secure the circuit pack.
2. Apply a constant pressure to gently pull the locking levers outward unlocking the latches. Do not remove the circuit pack.

   Result: If the circuit pack is the active circuit pack for transmission and timing, the system performs an automatic protection switch and subsequent transmission hits (less than 60 ms) will occur.

8 Remove the optical cables from the pack.

9 **Important!** The LNW59 OC-192 OLIU circuit pack may be equipped with up to two pluggable transmission modules. However, pluggable transmission modules are *not* required when the LNW59 OC-192 OLIU circuit pack is used in headless, optics-free, switch applications.

The LNW82 OLIU circuit pack may be equipped with a mix of up to eight OC-3/12/48 pluggable transmission modules. However, pluggable transmission modules are *not* required when the LNW82 OLIU circuit pack is used in headless, optics-free, switch applications.

The LNW202 OC-48, LNW203 OC-12, and LNW502 OC-192 OLIU circuit packs may be equipped with one pluggable transmission module.

The LNW504 OLIU circuit pack may be equipped with up to four OC-192 pluggable transmission modules or up to three OC–192 pluggable transmission modules and up to four OC-48 pluggable transmission modules. However, pluggable transmission modules are *not* required when the LNW504 OLIU circuit pack is used in headless, optics-free, switch applications.

If required, remove any pluggable transmission modules from the OLIU circuit pack .

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

10 Pull the locking levers to disengage the circuit pack from the backplane connector and draw the circuit pack out of the Main Slot.

11 **Important!** Pluggable transmission modules are shipped with a dust cover installed into the optical ports to maintain cleanliness during storage and/or transportation. It is recommended that the dust cover be kept in place to maintain cleanliness until the optical fiber is connected. With proper care and handling, cleaning the pluggable transmission modules should not be necessary.

If required, clean the pluggable transmission module.

Reference: Procedure 6-12: "Clean optical pluggable transmission module" (p. 6-160)

12 **Important!** The LNW121B-159B OLIU circuit packs are DA'ed and are no longer available.

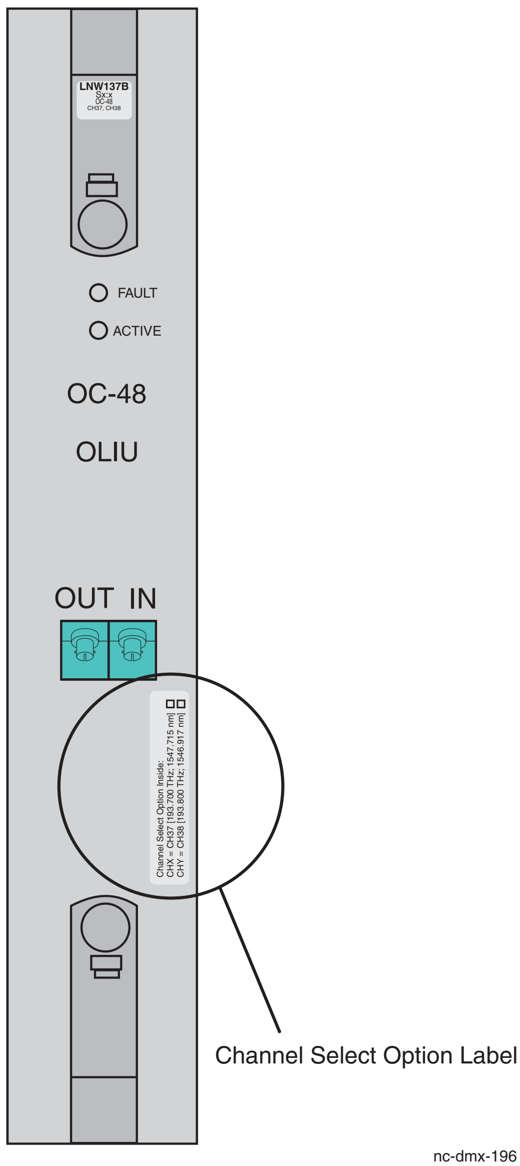
Are you replacing an LNW121B-159B or LNW221-259 OLIU circuit pack?

If...	Then...
Yes	Continue with Step 13.
No	Proceed to Step 16.

13 From your work orders, determine the wavelength that you wish to set on the LNW121B-LNW159B or LNW221-LNW259 circuit pack. Use the Channel Select Option Label on the faceplate of the circuit pack to determine the correct channel.

Example: From the Channel Select Option Label on the faceplate of the LNW137B (Figure 6-8, "Channel select option label on LNW137B" (p. 6-53)), we determine that for the desired CH37 wavelength (193.700 THz; 1547.715 nm), we must select CH X.

Figure 6-8 Channel select option label on LNW137B



14 If you are installing an...

- LNW121B-159B (Figure 6-9, “Jumper settings for LNW121B-159B” (p. 6-54))
  - Set the channel selection jumper on your circuit pack to either **CH X** or **CH Y** for your desired wavelength/channel.
  - Set the enhanced/normal jumper on your circuit pack to **Enhanced** (switch fabric can cross-connect VT across any 12 STS-1s). **Normal** (switch fabric can cross-connect VT across any 6 STS-1s) is not supported in Release 6.0.

  LNW221-259 (Figure 6-10, “Jumper settings for LNW221-259” (p. 6-55))
  - Set the channel selection jumper on your circuit pack to either **CH X** or **CH Y** for your desired wavelength/channel.

Figure 6-9 Jumper settings for LNW121B-159B

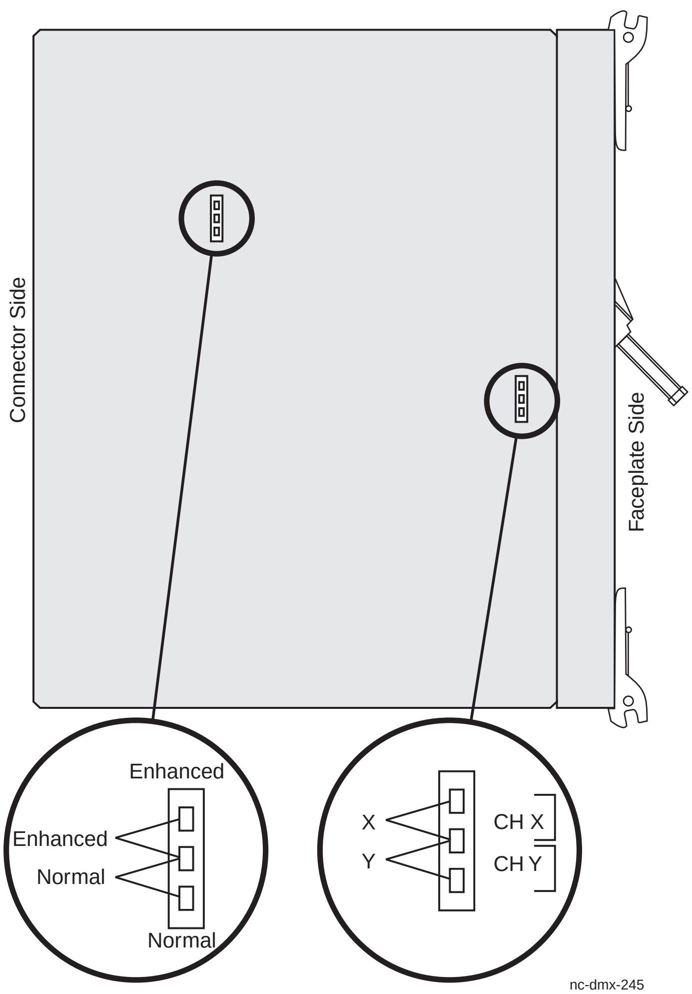
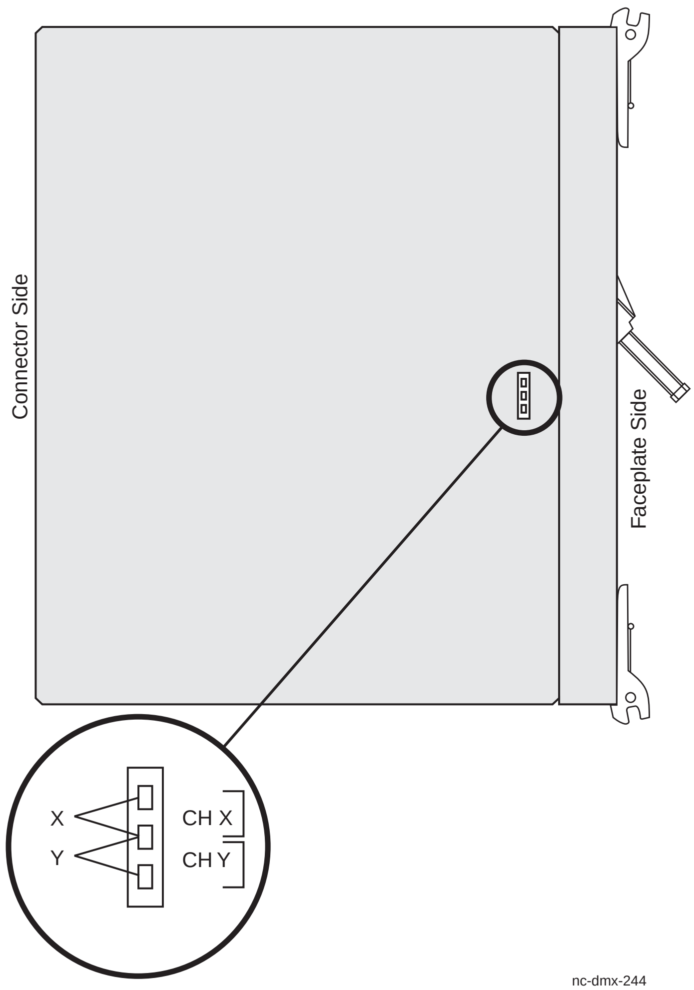


Figure 6-10 Jumper settings for LNW221-259



15 Using an erasable marker or pencil, check the appropriate box on the Channel Select Option Label (Figure 6-8, "Channel select option label on LNW137B" (p. 6-53)) that corresponds to your jumper setting.

Important! This label is the only means available to identify the wavelength selected when the pack is fully-seated and/or in-service.

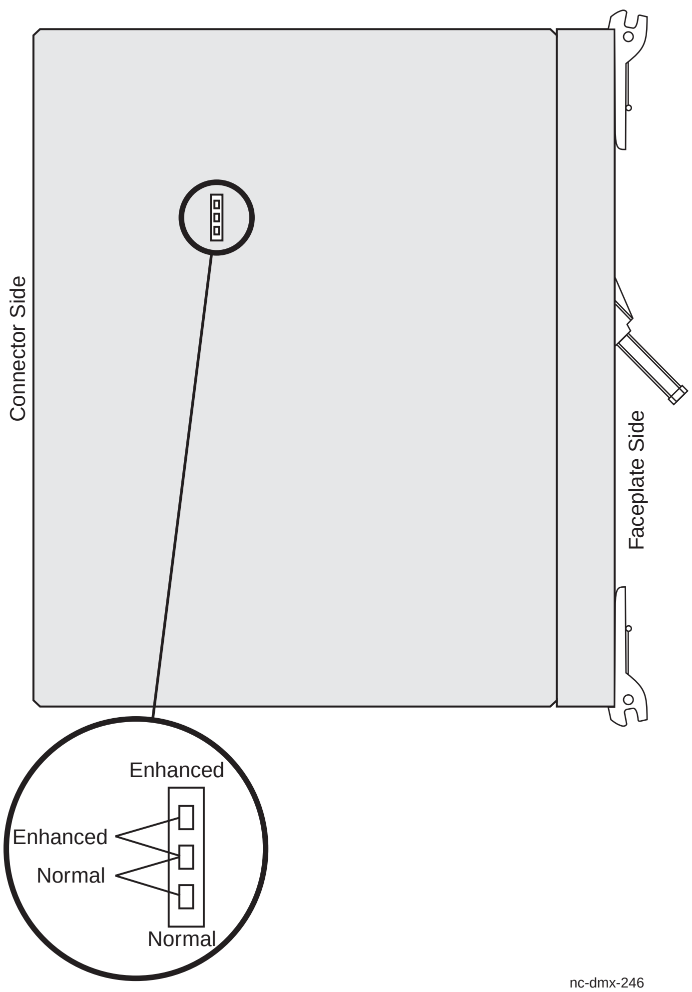
16 **Important!** The LNW26B, LNW28, LNW77, and LNW121B-159B OLIU circuit packs are DA'ed and are no longer available.

Are you installing an LNW26B, LNW28, LNW77, LNW121B-159B OLIU circuit pack?

If...	Then...
Yes	Continue with Step 17.
No	Proceed to Step 18.

17 Set the enhanced/normal jumper on your circuit pack to **Enhanced** (switch fabric can cross-connect VT across any 12 STS-1s). **Normal** (switch fabric can cross-connect VT across any 6 STS-1s) is not supported in Release 6.0. See Figure 6-11, "Jumper settings for enhanced mode" (p. 6-56).

Figure 6-11 Jumper settings for enhanced mode



18 Seat the replacement OLIU circuit pack in the vacant slot (M1 or M2) by applying steady pressure to both faceplate latches.

Result: For non-VLF OLIU circuit packs, the **FAULT** LED lights for approximately 20 seconds then goes off, indicating successful installation.

For VLF OLIU circuit packs, the **FAULT** LED lights for approximately 10 minutes then goes off, indicating successful installation.

MJ or MN and NE alarm LEDs on the SYSCTL circuit pack light when an OLIU circuit pack is installed. (Firmware updates may take place that add additional wait time.)

Select **View** → **Refresh System View** and the circuit pack appears in the *WaveStar*® CIT System View indicating successful installation.

19 **Important!** The LNW59 OC-192 OLIU circuit pack may be equipped with up to two pluggable transmission modules. However, pluggable transmission modules are *not* required when the LNW59 OC-192 OLIU circuit pack is used in headless, optics-free, switch applications.

The LNW82 OLIU circuit pack may be equipped with a mix of up to eight OC-3/12/48 pluggable transmission modules. However, pluggable transmission modules are *not* required when the LNW82 OLIU circuit pack is used in headless, optics-free, switch applications.

The LNW202 OC-48, LNW203 OC-12, and LNW502 OC-192 OLIU circuit packs may be equipped with one pluggable transmission module.

The LNW504 OLIU circuit pack may be equipped with up to four OC-192 pluggable transmission modules or up to three OC–192 pluggable transmission modules and up to four OC-48 pluggable transmission modules. However, pluggable transmission modules are *not* required when the LNW504 OLIU circuit pack is used in headless, optics-free, switch applications.

If required, install the pluggable transmission modules.

Reference: Procedure 6-8: “Replace pluggable transmission module” (p. 6-71)

20 Measure the optical receive power of the receive fiber using an optical power meter. Select the appropriate LBO to attenuate the receive signal to the middle of the allowable optical receive power range. (Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Applications and Planning Guide, 365-372-300* for the SONET optical specifications of the replacement circuit pack.)

21 Ensure all optical fiber connectors and couplings are properly cleaned on the replacement OLIU circuit pack.

Important! Signal performance may be degraded if the connections and couplings are not cleaned properly.

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

22 Reconnect the optical cables.

Result: **FAULT** LED goes off.

23 From the System View menu, click the **Alarm List** button to obtain an *NE Alarm List*. Verify that no alarms are present for the installed circuit pack.

If required, refer to the appropriate procedure to clear any alarms.

24 From the System View menu, use **View** → **Equipment** to access the circuit pack/port parameters for the circuit pack just installed and verify that the parameters are intact.

If required, refer to the appropriate procedure in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* to change any circuit pack/port parameters.

END OF STEPS

Procedure 6-6: Replace low-speed function unit OLIU circuit pack

Overview

Use this procedure to replace a low-speed OLIU circuit pack. These circuit packs are installed in Function Unit slots (A1/A2, B1/B2, C1/C2, D1/D2), and Growth Unit slots (G1/G2).

Required equipment

In addition to the equipment listed in "Required equipment" (p. 6-3), optical loopback cables, LBOs, and optical fiber cleaning tools may also be required if loopbacks are performed.

Use only Alcatel-Lucent Approved Class 1 SFP transceivers. Refer to the list of pluggable transmission modules in Procedure 6-8: "Replace pluggable transmission module" (p. 6-71).

Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*, as required, when removing and/or installing pluggable transmission modules.

> **Important!** If responses are not correct when replacing the OLIU circuit pack, check the connections. If the connections are correct, replace the OLIU circuit pack with the wrong response. (The red **FAULT** LED normally flashes when an OLIU circuit pack is monitored and there is no signal present.)

Before you begin

Prior to performing this procedure:

1. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) information in Chapter 1, "Safety".
2. Ensure that the correct low-speed OC-3/OC-12/OC-48/OC-192 OLIU circuit pack is available for replacement.
3. If required, ensure that the correct pluggable transmission modules are available for replacement.
4. Obtain work instructions for this procedure.

Steps

Complete the following steps to replace low-speed OLIU circuit pack.

1 **Important!** Low-speed OLIU circuit packs have more than one optical port. Each individual optical port can be provisioned for 0x1Sn, UPSR, 1+1, or Optimized 1+1 applications.

From the System View menu, select **Reports** → **Status Lists** → **Port**. Click on the low-speed OLIU circuit pack to be replaced and **Select**. Observe the value of the *Switch State* parameter for each port. If the port *Switch State* parameter is *active*, the port is active for transmission. Record any active ports and click **Close**.

2 Are there *active* ports on the low-speed OLIU circuit pack that you wish to replace?

If...	Then...
Yes	Continue with Step 3.
No	Proceed to Step 7.

3 To determine the protection groups associated with the active port(s) select **View** → **Equipment**. Expand the required low-speed OLIU circuit pack by clicking on the plus sign (+). Click on the required active port and **Select**. Observe the *Application* parameter to determine the type of protection.

To determine the protection group associated with other active ports, click on the required active port and **Select**. Click **Close** to exit.

4 If the *Application* parameter of any active ports is UPSR, at each node in the UPSR, select **Reports** → **Path Protection List** to verify that no *Forced* or *Lockout* path protection switches exist.

If required, clear any existing *Forced* or *Lockout* path protection switches using the **Fault** → **Protection Switch** → **Path Protection** → **Switch Type Clear** command.

5

If the Application parameter of the active port is...	Then perform a Forced protection switch...
1+1 or Optimized 1+1	to the standby line. Select **Fault** → **Protection Switch**. Click on the required *1+1 Line* protection group and **Select**. Select the *Forced* Switch Type and click **Apply**. A dialog box appears asking you to confirm executing this command. Click **Yes**. Repeat this step for all active 1+1 or Optimized 1+1 ports.
BLSR	to the protection tributaries on the companion port. Select **Fault** → **Protection Switch**. Click on the required *2F BLSR* protection group and **Select**. Select the *Force to Protection, Ring* Switch Type and click **Apply**. A dialog box appears asking you to confirm executing this command. Click **Yes**.

6

To verify that a...	Then...
1+1 or Optimized 1+1 line switch occurred,	Perform the following: 1. From the System View menu, select **View** → **Protection**. 2. Highlight the required 1+1 line protection group and click **Select**. 3. Verify that the port on the companion circuit pack is now active. 4. Verify that Switch Request State is *Forced Switch*.
BLSR line switch occurred,	Perform the following: 1. From the System View menu, select **View** → **Protection**. 2. Highlight the required 2F BLSR protection group and click **Select**. 3. Verify that Switch Request State is *Force to Protection, Ring*.

7 Remove the optical cables from the circuit pack.

8 **Important!** The LNW37 4OC-3 and LNW49 4OC-12 OLIU circuit packs may be equipped with up to four pluggable transmission modules. The LNW45 8OC-3 OLIU circuit packs may be equipped with up to eight pluggable transmission modules.

The LNW55 OC3/OC12/OC48 OLIU circuit packs may be equipped with a mix of up to twelve OC-3/12/48 pluggable transmission modules.

The LNW62 4OC-48 OLIU circuit packs may be equipped with up to four pluggable transmission modules.

The LNW402 OC-48 OLIU circuit packs may be equipped with one pluggable transmission module.

The LNW603 OC192 Very Large Fabric (VLF) tributary OLIU circuit packs may be equipped with one pluggable transmission module.

If required, remove any pluggable transmission modules from the OLIU circuit pack .

Reference: Procedure 6-8: “Replace pluggable transmission module” (p. 6-71)

9 Remove the circuit pack by grasping the inner edge of the locking-levers, and applying a constant pressure, pull the levers forward and remove the circuit pack.

10 **Important!** Pluggable transmission modules are shipped with a dust cover installed into the optical ports to maintain cleanliness during storage and/or transportation. It is recommended that the dust cover be kept in place to maintain cleanliness until the optical fiber is connected. With proper care and handling, cleaning the pluggable transmission modules should not be necessary.

If required, clean the pluggable transmission module.

Reference: Procedure 6-12: “Clean optical pluggable transmission module” (p. 6-160)

11 **Important!** The LNW421, LNW423, LNW431, LNW433, LNW435, LNW437, LNW443, LNW445, and LNW457 circuit packs are DA’ed and are no longer available.

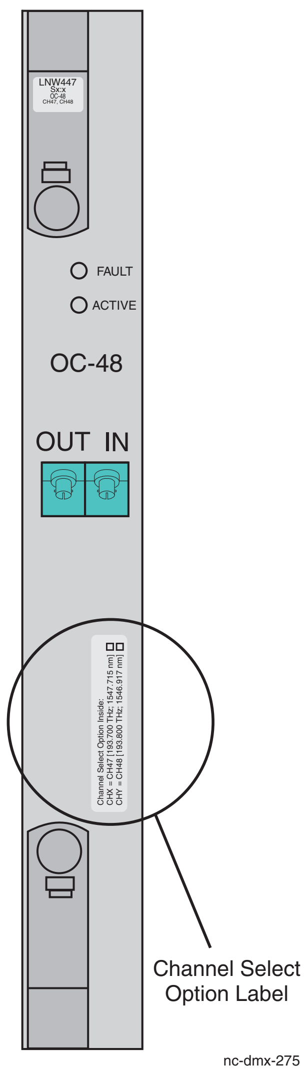
Are you installing an LNW421-459 OLIU circuit pack?

If...	Then...
Yes	Continue with Step 12.
No	Proceed to Step 15.

12 From your work orders, determine the wavelength that you wish to set on the LNW421-459 circuit pack. Use the Channel Select Option Label on the faceplate of the circuit pack to determine the correct channel.

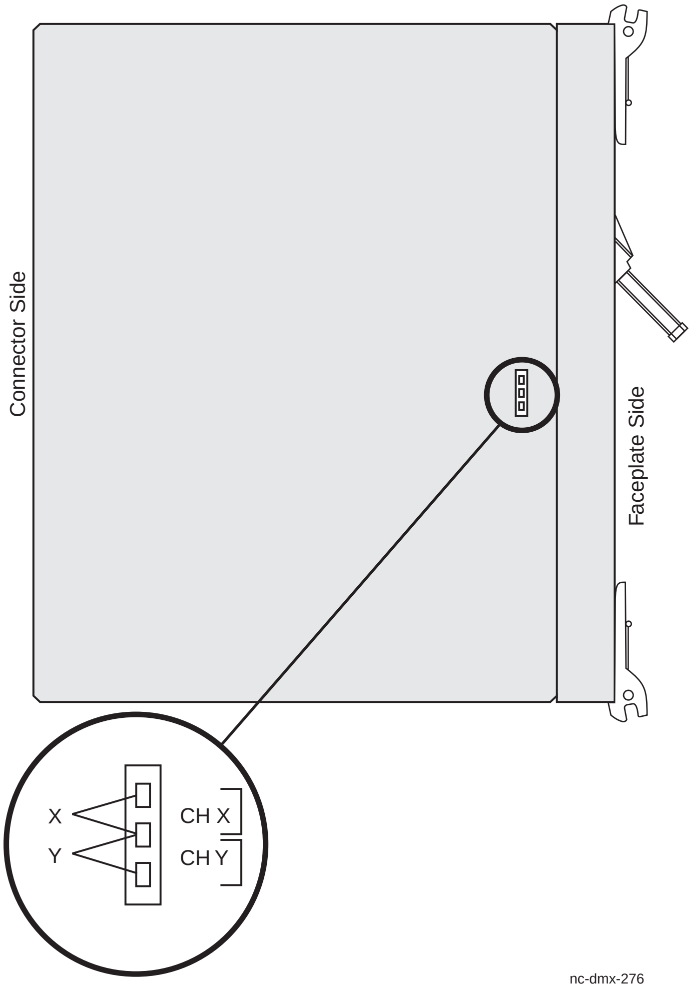
Example: From the Channel Select Option Label on the faceplate of the LNW447 (Figure 6-12, "Channel select option label on LNW447" (p. 6-63)), we determine that for the desired CH47 wavelength, we must select CH X.

Figure 6-12 Channel select option label on LNW447



13 Set the channel selection jumper on your circuit pack to either **CH X** or **CH Y** for your desired wavelength/channel (Figure 6-13, "Jumper settings for LNW421-459" (p. 6-64)).

Figure 6-13 Jumper settings for LNW421-459



14 Using an erasable marker or pencil, check the appropriate box on the Channel Select Option Label (Figure 6-12, "Channel select option label on LNW447" (p. 6-63)) that coresponds to your jumper setting.

Important! This label is the only means available to identify the wavelength selected when the pack is fully-seated and/or in-service.

15 Seat replacement OLIU circuit pack in the vacant slot by applying steady pressure to both faceplate latches.

Result: For LNW55 OC3/OC12/OC48, LNW62 4OC-48, and LNW603 OC-192 OLIU circuit packs, the **FAULT** LED lights for approximately 10 minutes then goes off, indicating successful installation.

For all other low-speed OLIU circuit packs, the **FAULT** LED lights for approximately 15 seconds then goes off, indicating successful installation.

Select **View** → **Refresh System View** and the circuit pack appears in the *WaveStar*® CIT System View indicating successful installation.

If both the original OLIU circuit pack and the replacement OLIU circuit pack fail when no other transmission circuit packs are installed in the shelf, replace the SYSCTL circuit pack. Refer to Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99).

16 **Important!** The LNW37 4OC-3 and LNW49 4OC-12 OLIU circuit packs may be equipped with up to four pluggable transmission modules. The LNW45 8OC-3 OLIU circuit packs may be equipped with up to eight pluggable transmission modules.

The LNW55 OC3/OC12/OC48 OLIU circuit packs may be equipped with a mix of up to twelve OC-3/12/48 pluggable transmission modules.

The LNW62 4OC-48 OLIU circuit packs may be equipped with up to four pluggable transmission modules.

The LNW402 OC-48 OLIU circuit packs may be equipped with one pluggable transmission module.

The LNW603 OC192 Very Large Fabric (VLF) tributary OLIU circuit packs may be equipped with one pluggable transmission module.

If required, install the pluggable transmission modules.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

17 Measure the optical receive power of the receive fiber using an optical power meter. Select the appropriate LBO to attenuate the receive signal to the middle of the allowable optical receive power range. (Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Applications and Planning Guide, 365-372-300* for the SONET optical specifications of the replacement circuit pack.)

18 Ensure all optical fiber connectors and couplings are properly cleaned on the replacement OLIU.

Important! Signal performance may be degraded if the connections and couplings are not cleaned properly.

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

19 Reconnect the optical cables.

Result: **FAULT** LED goes off.

20 If required, clear any Forced 1+1 or Optimized 1+1 line protection switch(es) performed in Step 5. Select **Fault** → **Protection Switch**. Click on the required *1+1 Line* protection group and **Select**. Select the *Reset* Switch Type and click **Apply**.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes**.

Repeat this step to clear all Forced 1+1 or Optimized 1+1 line protection switches.

21 If required, clear any BLSR Force to Protection, Ring protection switch(es) performed in Step 5. Select **Fault** → **Protection Switch**. Click on the required *2F BLSR* protection group and **Select**. Select the *Clear* Switch Type and click **Apply**.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes**.

22

To verify that a...	Then...
1+1 or Optimized 1+1 line switch cleared,	Perform the following: 1. From the System View menu, select **View** → **Protection**. 2. Highlight the required 1+1 line protection group and click **Select**. 3. Verify that Switch Request State is *No Request*.
BLSR line switch cleared,	Perform the following: 1. From the System View menu, select **View** → **Protection**. 2. Highlight the required 2F BLSR protection group and click **Select**. 3. Verify that Switch Request State is *No Request*.

Result: If Switch Request State reads Signal Failure or Signal Degrade, there is a higher priority switch request in place.

23 From the System View menu, click the **Alarm List** button to obtain an *NE Alarm List*. Verify that no alarms are present for the installed circuit pack.

If required, refer to the appropriate procedure to clear any alarms.

24 From the System View menu, use **View** → **Equipment** to access the circuit pack/port parameters for the circuit pack just installed and verify that the parameters are intact.

If required, refer to the appropriate procedure in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* to change any circuit pack/port parameters.

END OF STEPS

Procedure 6-7: Replace Ethernet/Data circuit pack

Overview

Use this procedure to replace the following Ethernet and Data circuit packs:

- LNW63 GBE PL Gigabit Ethernet circuit pack
- LNW64 GBE PL Gigabit Ethernet circuit pack
- LNW66 10/100 Base TX Fast Ethernet circuit pack
- LNW67 1GbE-SX Gigabit Ethernet circuit pack
- LNW68 1GbE-LX Gigabit Ethernet circuit pack
- LNW70 100/1G FXS Gigabit Ethernet circuit pack
- LNW71 10/100-PL Fast Ethernet circuit pack
- LNW73/LNW73C FC Fibre Channel circuit pack
- LNW74 10/100T/F Enhanced Private Line Ethernet circuit pack
- LNW78 100/1G FSR Gigabit Ethernet circuit pack
- LNW87 FE/GBE PL 4-Port Gigabit Ethernet and Fast Ethernet Private Line circuit pack
- LNW170 100/1G FXS Gigabit Ethernet circuit pack

  Important! You must replace an LNW67 with an LNW67 and an LNW68 with an LNW68. The LNW67 and LNW68 are interchangeable, except that the LNW68 is equipped with short reach optics and the LNW68 is equipped with long reach optics.

Required equipment

Use only Alcatel-Lucent Approved Class 1 SFP transceivers. Refer to the list of pluggable transmission modules in Procedure 6-8: "Replace pluggable transmission module" (p. 6-71).

Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*, as required, when removing and/or installing pluggable transmission modules.

Before you begin

Prior to performing this procedure:

1. Refer to "Required equipment" (p. 6-3) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) information in Chapter 1, "Safety".
3. Obtain work instructions for this procedure.

4. Ensure that the appropriate circuit pack is available for replacement.
5. If required, ensure that the correct pluggable transmission modules are available for replacement.

Steps

Complete the following steps to replace an Ethernet/Data circuit pack.

1 If required, remove the cables from the circuit pack.

2 **Important!** The LNW63, LNW64, LNW70, LNW73/LNW73C, LNW74, LNW78, and LNW170 circuit packs may be equipped with pluggable transmission modules.

If required, remove any pluggable transmission modules from the circuit pack.

Reference: Procedure 6-8: “Replace pluggable transmission module” (p. 6-71)

3 Remove the required circuit pack by grasping the inner edge of the locking-levers, and applying a constant pressure, pull the levers forward and remove the circuit pack.

4 Ensure that all optical fiber connectors and couplings are properly cleaned on the replacement circuit pack.

Important! Signal performance may be degraded if the connections and couplings are not cleaned properly.

Reference: Procedure 6-11: “Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)” (p. 6-151)

5 **Important!** Pluggable transmission modules are shipped with a dust cover installed into the optical ports to maintain cleanliness during storage and/or transportation. It is recommended that the dust cover be kept in place to maintain cleanliness until the optical fiber is connected. With proper care and handling, cleaning the pluggable transmission modules should not be necessary.

If required, clean the optical pluggable transmission module.

Reference: Procedure 6-12: “Clean optical pluggable transmission module” (p. 6-160)

6 Seat the replacement circuit pack in vacated Function Unit slot.

Result: **FAULT** LED on the circuit pack lights. After approximately 60 seconds, the **ACTIVE** LED lights and the **FAULT** LED may go off. (Firmware updates may take place that add additional wait time.)

Select **View** → **Refresh System View** and the circuit pack appears in the *WaveStar*® CIT System View indicating successful installation.

If both the original circuit pack and the replacement circuit pack fail when no other transmission circuit packs are installed in the shelf, replace the SYSCTL circuit pack. Refer to Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99).

7 **Important!** The LNW63, LNW64, LNW70, LNW73/LNW73C, LNW74, LNW78, and LNW170 circuit packs may be equipped with pluggable transmission modules.

If required, install the pluggable transmission modules.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

8 If required, reconnect the cables.

Result: The circuit pack **FAULT** LED or port LED associated with the pluggable transmission module stops flashing.

9 Ensure that a 177D apparatus blank or an LNW98 Detectable apparatus blank is present in the unequipped companion Function Unit slot.

10 From the System View menu, click the **Alarm List** button to obtain an *NE Alarm List*. Verify that no alarms are present for the installed circuit pack.

If required, refer to the appropriate procedure to clear any alarms.

11 From the System View menu, use **View** → **Equipment** to access the circuit pack/port parameters for the circuit pack just installed and verify that the parameters are intact.

If required, refer to the appropriate procedure in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* to change any circuit pack/port parameters.

END OF STEPS

Procedure 6-8: Replace pluggable transmission module

Overview

Use this procedure to replace a pluggable transmission module in a circuit pack.

Required equipment

Use only the following Alcatel-Lucent Approved Class 1 SFP/XFP transceivers.

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
EM1G//EMFE 1000BASE-T//100BASE-T	BASE-T-C1 109565549	10 Mb/s, 100 Mb/s and GbE, Copper, SFP TRCVR	LNW63 LNW64 LNW70/LNW170 LNW78 LNW87
OM155 1.3IR1	OC3IR1-I1 109453894	OC3 IR1, SM, 1310 nm, 15 km, SFP TRCVR	LNW37 LNW45 LNW55 LNW82 LNW705
OM155 1.3LR1	OC3LR1-I1 109453886	OC3 LR1, SM, 1310 nm, 40 km, SFP TRCVR	LNW37 LNW45 LNW55 LNW82 LNW705
OM155 1.3SR1	S155I2 109602599	OC-3 SR-1/STM-1, SM, 1310 nm, 2 km, SFP TRCVR	LNW37 LNW45 LNW55 LNW82 LNW705
OM155//OM622 //2.5G 1.3IR1//1.3IR1// 1.3IR1	OC3X12X48-IR1-I1 109708131	OC3/STM1/OC12/ STM4/OC48/STM16, 1310nm, 15 km, SFP TRCVR	LNW55 LNW82

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
OM155//OM622// 2.5G 1.3LR1//1.3LR1// 1.3LR1	OC3X12X48-LR1-I1 109708149	OC3/STM1/OC12/ STM4/OC48/STM16, 1310nm, 40km, 15 km, SFP TRCVR	LNW55 LNW82
OM622 1.3IR1	OC12IR1-I1 109453902	OC12 IR1, SM, 1310 nm, 15 km, SFP TRCVR	LNW49 LNW55 LNW82 LNW203 LNW705
OM622 1.3LR1	OC12LR1-I1 109467522	OC12 LR1, SM, 1310 nm, 40 km, SFP TRCVR	LNW49 LNW55 LNW82 LNW203 LNW705
OM622 1.5LR2	OC12LR2-I1 109604447	OC12 LR2, SM, 1550 nm, 80 km, SFP TRCVR	LNW49 LNW55 LNW82 LNW203 LNW705
OM155//OM622/ CWDM-LR	S622C47EL 109664086	OC-3/STM-1 or OC-12/STM-4 CWDM, 1471 nm, SFP TRCVR	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705
OM155//OM622/ CWDM-LR	S622C49EL 109664094	OC-3/STM-1 or OC-12/STM-4 CWDM, 1491 nm, SFP TRCVR	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
OM155//OM622/ CWDM-LR	S622C51EL 109664102	OC-3/STM-1 or OC-12/STM-4 CWDM, 1511 nm, SFP TRCVR	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705
OM155//OM622/ CWDM-LR	S622C53EL 109664110	OC-3/STM-1 or OC-12/STM-4 CWDM, 1531 nm, SFP TRCVR	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705
OM155//OM622/ CWDM-LR	S622C55EL 109664128	OC-3/STM-1 or OC-12/STM-4 CWDM, 1551 nm, SFP TRCVR	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705
OM155//OM622/ CWDM-LR	S622C57EL 109664136	OC-3/STM-1 or OC-12/STM-4 CWDM, 1571 nm, SFP TRCVR	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705
OM155//OM622/ CWDM-LR	S622C59EL 109664144	OC-3/STM-1 or OC-12/STM-4 CWDM, 1591 nm, SFP TRCVR	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
OM155//OM622/ CWDM-LR	S622C61EL 109664151	OC-3/STM-1 or OC-12/STM-4 CWDM, 1611 nm, SFP TRCVR	LNW37 LNW45 LNW49 LNW55 LNW82 LNW705
OM1G 1000BASE-ZX	1000BASE-ZX-I1 109541862	GbE SM 1550 nm 1000BASE-ZX SFP TRCVR	LNW63 LNW64 LNW70/LNW170 LNW78 LNW87
OM1G//OMFC 1000BASE-LX//100/200-SM-LL-L-I	GE-1X2XFC-LX-C1 109527804	GbE SM 1310 nm 1XFC/2XFC 1000BASE-LX SFP TRCVR	LNW64 LNW70/LNW170 LNW73/73C LNW78 LNW87
OM1G//OMFC 1000BASE-LX//100/200-SM-LL-L-I	GE-1X2XFC-LX-I1 109568782	GbE SM 1310 nm 1XFC/2XFC 1000BASE-LX SFP TRCVR	LNW63 LNW64 LNW70/LNW170 LNW73/73C LNW78 LNW87 LNW705
OM1G//OMFC 1000BASE-SX//100/200-M5/M6-SN-S	GE-1X2XFC-SX-C1 109527796	GbE MM 850 nm 1XFC/2XFC 1000BASE-SX SFP TRCVR	LNW64 LNW70/LNW170 LNW73/73C LNW78 LNW87

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
OM1G//OMFC 1000BASE-SX//100/200-M5/M6-SN-S	GE-1X2XFC-SX-I1 109570606	GbE MM 850 nm 1XFC/2XFC 1000BASE-SX SFP TRCVR	LNW63 LNW64 LNW70/LNW170 LNW73/73C LNW78 LNW87 LNW705
OM2.5G 1.3LR1	OC48LR1-I1 109493528	OC48 LR1, SM, 1310 nm, 40 km, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504 LNW705
OM2.5G 1.5LR2	OC48LR2-I1 109504431	OC48 LR2, SM, 1550 nm, 80 km, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504 LNW705
OM2.5G 1.3SR1	OC48SR1-I1 109564518	OC48 SR1, SM, 1310 nm, 2 km, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW705
OM2.5G 1.5LR2	S2D23C6 109610378	OC-48 /STM-16/OTU1 DWDM, 192.3 THz, 1558.983 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
OM2.5G 1.5LR2	S2D25C6 109610394	OC-48 /STM-16/OTU1 DWDM, 192.5 THz, 1557.363 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G 1.5LR2	S2D27C6 109610410	OC-48 /STM-16/OTU1 DWDM, 192.7 THz, 1555.747 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G 1.5LR2	S2D31C6 109610451	OC-48 /STM-16/OTU1 DWDM, 193.1 THz, 1552.524 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G 1.5LR2	S2D33C6 109610477	OC-48 /STM-16/OTU1 DWDM, 193.3 THz, 1550.918 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G 1.5LR2	S2D35C6 109610493	OC-48 /STM-16/OTU1 DWDM, 193.5 THz, 1549.315 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
OM2.5G 1.5LR2	S2D37C6 109610519	OC-48 /STM-16/OTU1 DWDM, 193.7 THz, 1547.715 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G 1.5LR2	S2D45C6 109610600	OC-48 /STM-16/OTU1 DWDM, 194.5 THz, 1541.349 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G 1.5LR2	S2D47C6 109610626	OC-48 /STM-16/OTU1 DWDM, 194.7 THz, 1539.766 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G 1.5LR2	S2D49C6 109610642	OC-48 /STM-16/OTU1 DWDM, 194.9 THz, 1538.186 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G 1.5LR2	S2D53C6 109610691	OC-48 /STM-16/OTU1 DWDM, 195.3 THz, 1535.036 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
OM2.5G 1.5LR2	S2D55C6 109610717	OC-48 /STM-16/OTU1 DWDM, 195.5 THz, 1533.465 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G 1.5LR2	S2D59C6 109610766	OC-48 /STM-16/OTU1 DWDM, 195.9 THz, 1530.334 nm, SFP TRCVR	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G/SL-16.2	S2G7C47LI 1AB402160002	OC48/STM16 CWDM 1471 nm, SFP TRCVR S-C8L1-1D2 : S-C8L1-1D5	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G/SL-16.2	S2G7C49LI 1AB402160003	OC48/STM16CWDM 1491 nm, SFP TRCVR S-C8L1-1D2 : S-C8L1-1D5	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G/SL-16.2	S2G7C51LI 1AB402160004	OC48/STM16 CWDM 1511 nm, SFP TRCVR S-C8L1-1D2 : S-C8L1-1D5	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
OM2.5G/SL-16.2	S2G7C53LI 1AB402160005	OC48/STM16 CWDM 1531 nm, SFP TRCVR S-C8L1-1D2 : S-C8L1-1D5	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G/SL-16.2	S2G7C55LI 1AB402160006	OC48/STM16 CWDM 1551 nm, SFP TRCVR S-C8L1-1D2 : S-C8L1-1D5	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G/SL-16.2	S2G7C57LI 1AB402160007	OC48/STM16CWDM 1571 nm, SFP TRCVR S-C8L1-1D2 : S-C8L1-1D5	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G/SL-16.2	S2G7C59LI 1AB402160008	OC48/STM16 CWDM 1591 nm, SFP TRCVR S-C8L1-1D2 : S-C8L1-1D5	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504
OM2.5G/SL-16.2	S2G7C61LI 1AB402160009	OC48/STM16 CWDM 1611 nm, SFP TRCVR S-C8L1-1D2 : S-C8L1-1D5	LNW55 LNW62 LNW82 LNW202 LNW402 LNW504

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
OM10G 1.5IR2 (S-64.2b)	OC192IR2-C1 109537563	OC192 IR2, SM, 1550 nm, 40 km, XFP TRCVR	LNW59 LNW502 LNW504 LNW603 LNW705
OM10G 1.5IR2 (S-64.2b)	OC192IR2-I1 109586479	OC192 IR2, SM, 1550 nm, 40 km, XFP TRCVR	LNW59 LNW705
OM10G 1.5LR2 (P1L1-2D2)	OC192LR2-C1 109537555	OC192 LR2, SM, 1550 nm, 80 km, XFP TRCVR	LNW59 LNW502 LNW504 LNW603 LNW705
OM10G 1.3SR1 (I-64.1)	OC192SR1-C1 109537902	OC192 SR1, SM, 1310 nm, 2 km, XFP TRCVR	LNW59 LNW502 LNW504 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G21C5 109615005	OC-192/STM-64/OTU2 DWDM, 192.1 THz, 1560.606 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G22C5 109615013	OC-192/STM-64/ OTU2 DWDM, 192.2 THz, 1559.794 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G23C5 109615021	OC-192/STM-64/ OTU2 DWDM, 192.3 THz, 1558.983 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G24C5 109615039	OC-192/STM-64/ OTU2 DWDM, 192.4 THz, 1558.173 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
OM10G DWDMLR (DW100U-2AxC(F))	X10G25C5 109615047	OC-192/STM-64/ OTU2 DWDM, 192.5 THz, 1557.363 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G26C5 109615054	OC-192/STM-64/ OTU2 DWDM, 192.6 THz, 1556.555 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G27C5 109615062	OC-192/STM-64/ OTU2 DWDM, 192.7 THz, 1555.747 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G28C5 109615070	OC-192/STM-64/ OTU2 DWDM, 192.8 THz, 1554.940 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G31C5 109615104	OC-192/STM-64/ OTU2 DWDM, 193.1 THz, 1552.524 nm, XFP TRCVR	LNW59 LNW502 LNW504 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G33C5 109615120	OC-192/STM-64/ OTU2 DWDM, 193.3 THz, 1550.918 nm, XFP TRCVR	LNW59 LNW502 LNW504 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G35C5 109615146	OC-192/STM-64/ OTU2 DWDM, 193.5 THz, 1549.315 nm, XFP TRCVR	LNW59 LNW502 LNW504 LNW603 LNW705

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
OM10G DWDMLR (DW100U-2AxC(F))	X10G37C5 109615161	OC-192/STM-64/ OTU2 DWDM, 193.7 THz, 1547.715 nm, XFP TRCVR	LNW59 LNW502 LNW504 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G45C5 109615245	OC-192/STM-64/ OTU2 DWDM, 194.5 THz, 1541.349 nm, XFP TRCVR	LNW59 LNW502 LNW504 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G47C5 109615260	OC-192/STM-64/ OTU2 DWDM, 194.7 THz, 1539.766 nm, XFP TRCVR	LNW59 LNW502 LNW504 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G49C5 109615286	OC-192/STM-64/ OTU2 DWDM, 194.9 THz, 1538.186 nm, XFP TRCVR	LNW59 LNW502 LNW504 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G52C5 109615310	OC-192/STM-64/ OTU2 DWDM, 195.2 THz, 1535.822 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G53C5 109615328	OC-192/STM-64/ OTU2 DWDM, 195.3 THz, 1535.036 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G54C5 109615336	OC-192/STM-64/ OTU2 DWDM, 195.4 THz, 1534.250 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705

Name/ Qualifier	Pluggable Transmission Module Code/Comcode	Description	Compatible Circuit Packs
OM10G DWDMLR (DW100U-2AxC(F))	X10G55C5 109615344	OC-192/STM-64/ OTU2 DWDM, 195.5 THz, 1533.465 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G56C5 109615351	OC-192/STM-64/ OTU2 DWDM, 195.6 THz, 1532.681 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G57C5 109615369	OC-192/STM-64/ OTU2 DWDM, 195.7 THz, 1531.898 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G58C5 109615377	OC-192/STM-64/ OTU2 DWDM, 195.8 THz, 1531.116 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OM10G DWDMLR (DW100U-2AxC(F))	X10G59C5 109615385	OC-192/STM-64/ OTU2 DWDM, 195.9 THz, 1530.334 nm, XFP TRCVR	LNW59 LNW502 LNW603 LNW705
OMESCON MMF	ESCON-MM-I1 109523886	ESCON MM, 1310 nm SFP TRCVR	LNW73/73C
OMFE 100BASE-LX-SM	100BASE-LX-I1 109527812	100 Mb/s optical Fast Ethernet SFP TRCVR	LNW70/LNW170 LNW74 LNW78 LNW87
OMFE 100BASE-FX	100BASE-FX-I1 109703140	100 Mb/s optical Fast Ethernet SFP TRCVR	LNW70/LNW170 LNW74 LNW78 LNW87
OMFE 100BASE-ZX	100BASE-ZX-I1 109703157	100 Mb/s optical Fast Ethernet SFP TRCVR	LNW74 LNW87 LNW170

Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*, as required, when removing and/or installing pluggable transmission modules.

Before you begin

Prior to performing this procedure:

1. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) information in Chapter 1, "Safety".
2. Using office records and/or **View** → **Equipment**, determine the correct type of pluggable transmission module to be replaced.
3. Ensure that the correct pluggable transmission module is available for replacement.

Steps

Complete the following steps to replace a pluggable transmission module.

1

If replacing a pluggable transmission module in an...	Then...
optical OLIU circuit pack,	Continue with Step 2.
Ethernet or DATA circuit pack,	Proceed to Step 8.

2

Important! Low-speed OLIU circuit packs have more than one optical port. Each individual optical port can be provisioned for 1+1 (1+1, Optimized 1+1, or Bidirectional 1+1), 0x1Sn, or UPSR applications.

From the System View menu, select **Reports** → **Status Lists** → **Port**. Click on the required low-speed OLIU circuit pack with the pluggable transmission module to be replaced and **Select**. Observe the value of the *Switch State* parameter for the required port. If the port *Switch State* parameter is *active*, the port is active for transmission. Click **Close**.

3 Is the port *active* on the pluggable transmission module that you wish to replace?

If...	Then...
Yes	Continue with Step 4.
No	Proceed to Step 8.

4 To determine the protection group associated with the active port select **View** → **Equipment**. Expand the required low-speed OLIU circuit pack by clicking on the plus sign (+). Click on the required active port and **Select**. Observe the *Application* parameter to determine the type of protection. Click **Close** to exit.

5 If the *Application* parameter of any active ports is UPSR, at each node in the UPSR, select **Reports** → **Path Protection List** to verify that no *Forced* or *Lockout* path protection switches exist.

If required, clear any existing *Forced* or *Lockout* path protection switches using the **Fault** → **Protection Switch** → **Path Protection** → **Switch Type Clear** command.

6

If the Application parameter of the active port is...	Then perform a Forced protection switch...
1+1,	to the standby line. Select **Fault** → **Protection Switch**. Click on the required *1+1 Line* protection group and **Select**. Select the *Forced* Switch Type and click **Apply**. A dialog box appears asking you to confirm executing this command. Click **Yes**.
1+1_bidir,	to the standby line. Select **Fault** → **Protection Switch**. Click on the required *1+1_bidir line fn-{d,g}-{1-x}* protection group and **Select**. Select the *Forced* Switch Type and click **Apply**. A dialog box appears asking you to confirm executing this command. Click **Yes**.
1+1_optm,	to the standby line. Select **Fault** → **Protection Switch**. Click on the required *1+1_optm line fn-{d,g}-{1-x}* protection group and **Select**. Select the *Forced*Switch Type and click **Apply**. A dialog box appears asking you to confirm executing this command. Click **Yes**.

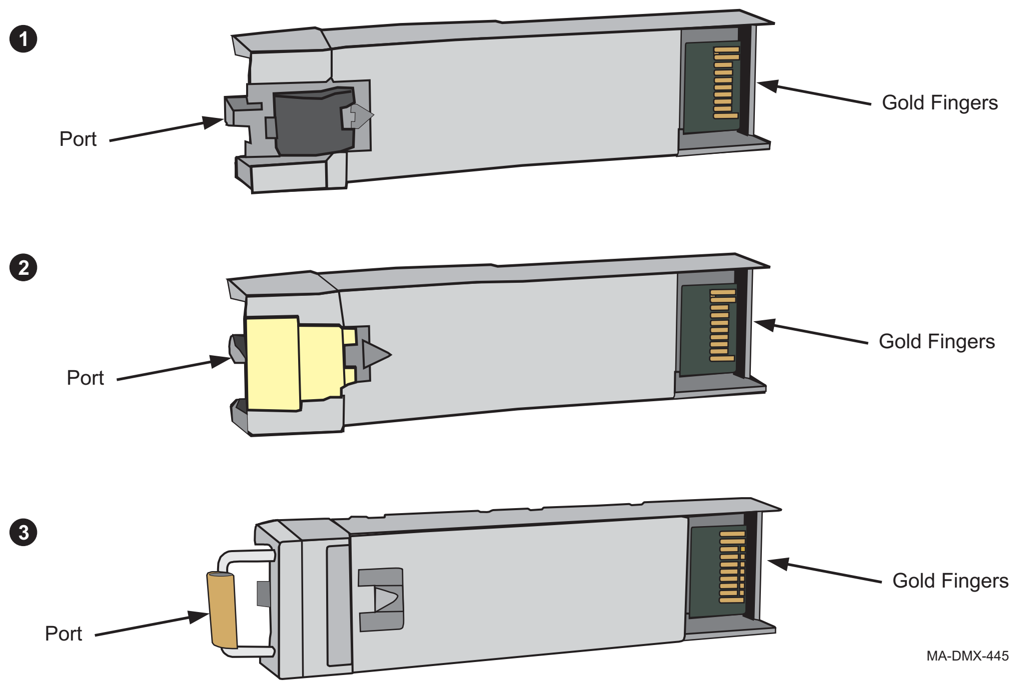
7 To verify that a 1+1 switch occurred, perform the following:

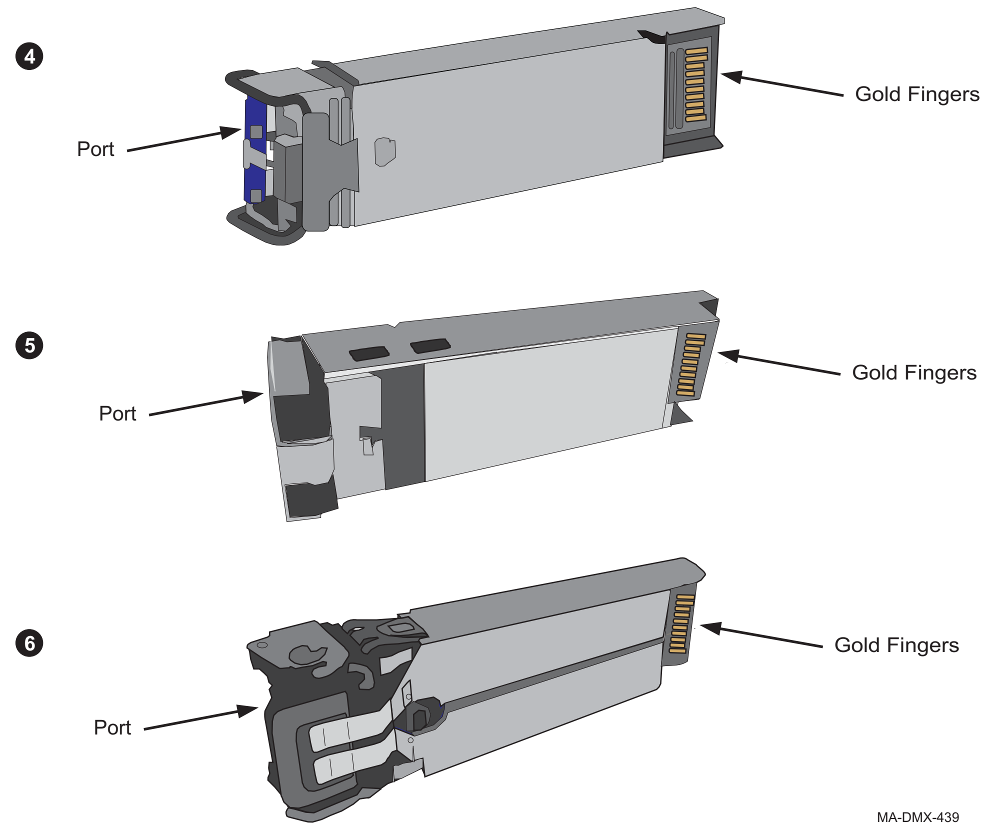
1. From the System View menu, select **View** → **Protection**.
2. Highlight the required 1+1, 1+1_optm, or 1+1_bidir line protection group and click **Select**.

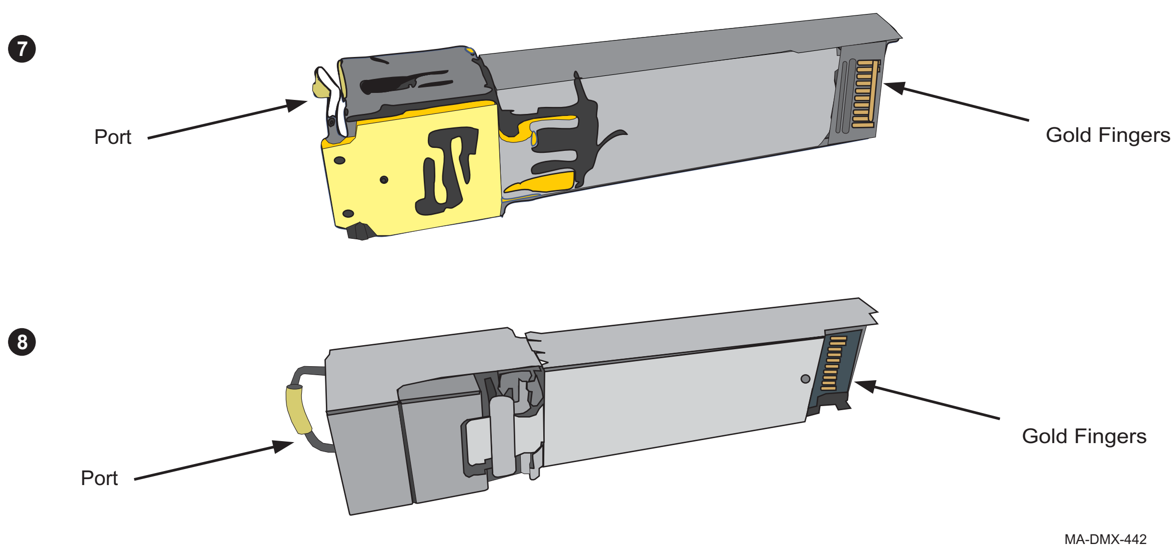
3. Verify that the port on the companion circuit pack is now active.
4. Verify that Switch Request State is *Forced Switch*.

8 Remove the cables from the required pluggable transmission module.

9 Referring to the figure below, determine the type of latching mechanism on the pluggable transmission module you have.




4
Port
Gold Fingers
5
Port
Gold Fingers
6
Port
Gold Fingers
MA-DMX-439


7
Port
Gold Fingers
8
Port
Gold Fingers
MA-DMX-442

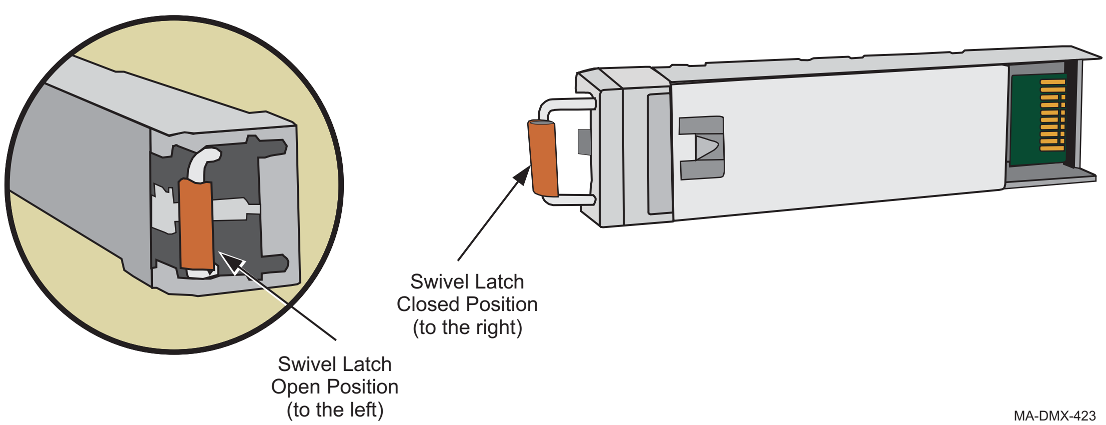
10 Referring to Step 9, what type of latching mechanism does your module have?

If...	Then...
Type 1 (optical)	Remove the required pluggable transmission module from the circuit pack by pushing the plastic tab on the side of the module toward the back of the shelf (away from you), then gripping the sides of the module, remove it from the socket. Proceed to Step 14.
Type 2 (optical)	Remove the required pluggable transmission module from the circuit pack by squeezing the plastic tab on the side of the module toward the left of the shelf, then gripping the sides of the module, remove it from the socket. Proceed to Step 14.
Type 3 (optical)	Continue with Step 11.
Type 4, 5, and 6 (optical)	Proceed to Step 13.
Type 7 and 8 (electrical)	Proceed to Step 13.

11 Before removing the module, the latch must be in the open position. Open the swivel latch and pull gently on the latch to remove the pluggable transmission module from the socket.

Figure 6-14, "Latch type 3 (opened and closed)" (p. 6-88) shows the open and closed position of the latch. Depending on your pluggable transmission module type, the appearance of the port opening and latch mechanism may vary.

Figure 6-14 Latch type 3 (opened and closed)

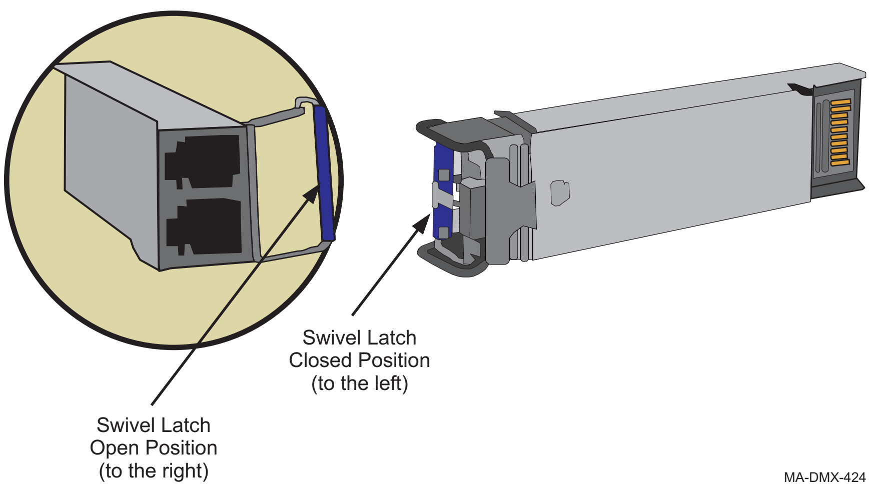


12 Proceed to Step 14.

13 Before removing the module, the latch must be in the open position. Open the swivel latch and pull gently on the latch to remove the pluggable transmission module from the socket.

Figure 6-15, "Latch type 4, 5, 6, 7, and 8 (opened and closed)" (p. 6-89) shows the open and closed position of the latch. Depending on your pluggable transmission module type, the appearance of the port opening and latch mechanism may vary.

Figure 6-15 Latch type 4, 5, 6, 7, and 8 (opened and closed)

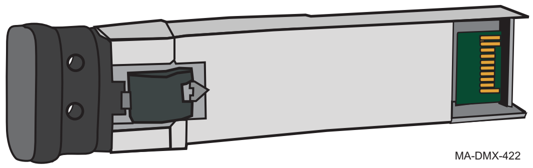


14 **Important!** It is recommended that dust covers be installed into the ports on optical pluggable transmission modules to maintain cleanliness until the cable is connected. Electrical pluggable transmission modules do not require dust covers.

If you just removed an optical pluggable transmission module, install dust covers into the ports to maintain cleanliness.

15 Before installing the replacement pluggable transmission module, hold the connector/latch-end of the module in your left hand with the gold fingers facing you. The module should be positioned in manner similar to Figure 6-16, "Pluggable transmission module with dust cover (optical only)" (p. 6-90).

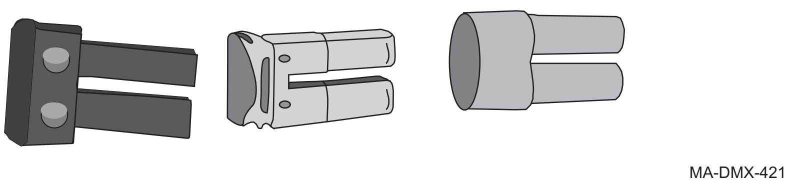
Figure 6-16 Pluggable transmission module with dust cover (optical only)



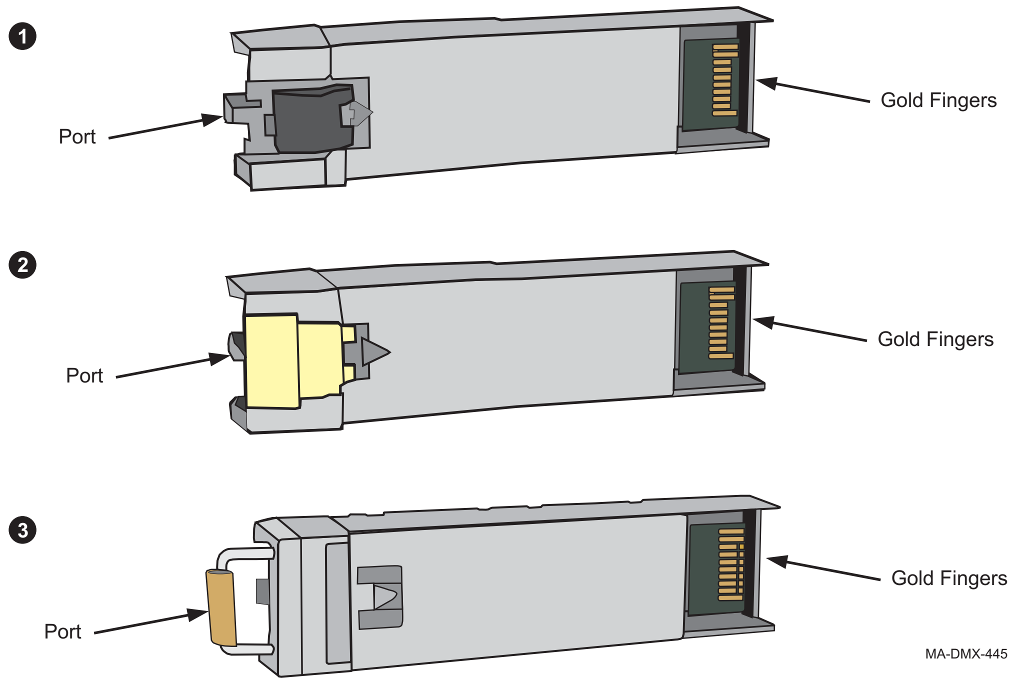
Important! Do not remove the dust cover unless you are ready to connect cabling or if you need to clean the module.

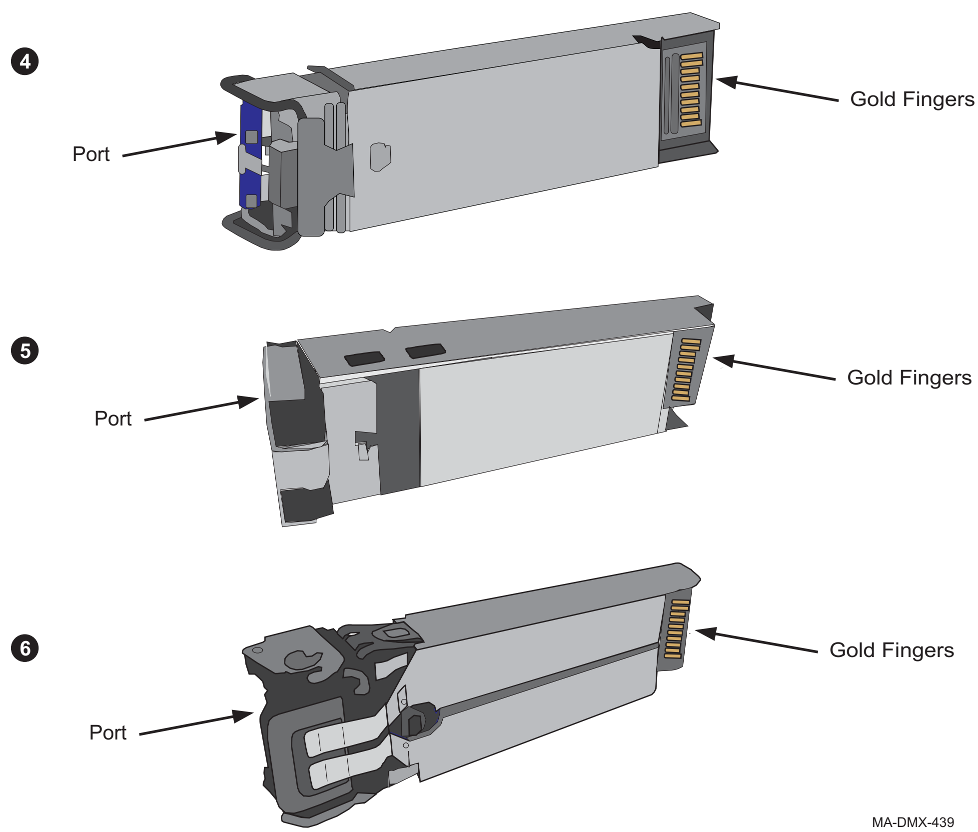
Dust covers There are a variety of different types of dust covers. Any of the following examples could be similar to the dust cover in your optical pluggable transmission module.

Figure 6-17 Examples of dust covers

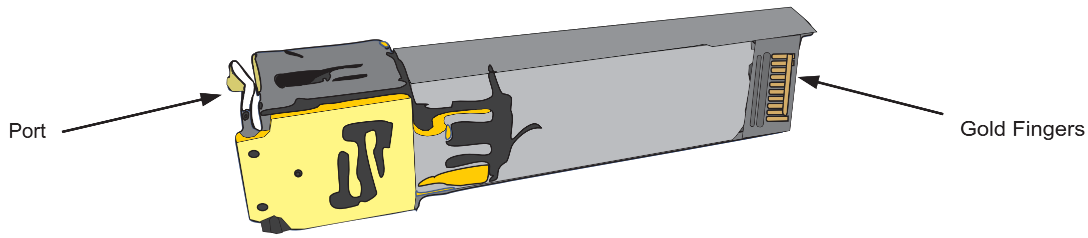


16 Referring to the figure below, determine the type of latching mechanism on the pluggable transmission module you have.

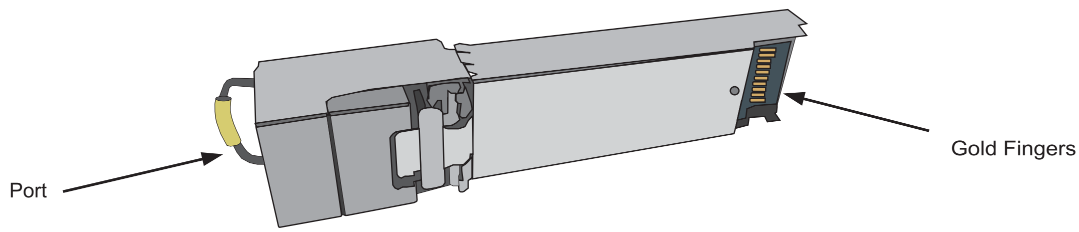

1
Port
Gold Fingers
2
Port
Gold Fingers
3
Port
Gold Fingers
MA-DMX-445


4
Port
Gold Fingers
5
Port
Gold Fingers
6
Port
Gold Fingers
MA-DMX-439

7



8



17 **Important!** Optical pluggable transmission modules are shipped with a dust cover installed into the optical ports to maintain cleanliness during storage and/or transportation. It is recommended that the dust cover be kept in place to maintain cleanliness until the optical fiber is connected. With proper care and handling, cleaning the pluggable transmission modules should not be necessary.

Electrical pluggable transmission modules do not require dust covers.

If required, clean the optical pluggable transmission module.

Reference: Procedure 6-12: "Clean optical pluggable transmission module" (p. 6-160)

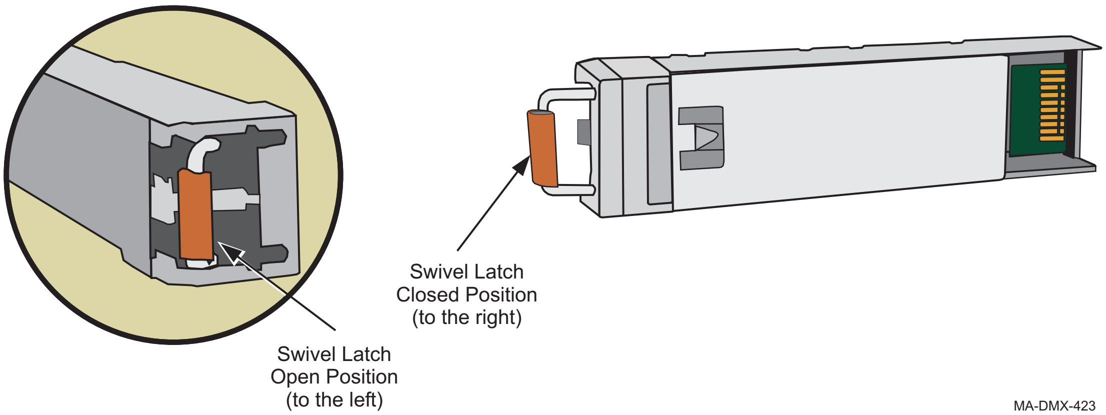
18 Referring to Step 16, what type of latching mechanism does your module have?

If...	Then...
Type 1 or 2 (optical)	Proceed to Step 22.
Type 3 (optical)	Continue with Step 19.
Type 4, 5 or 6 (optical)	Proceed to Step 21.
Type 7 or 8 (electrical)	Proceed to Step 21.

19 Before inserting the module, the latch must be in the closed position. On optical pluggable transmission modules, the latch is in the closed position when the dust cover is place.

Figure 6-18, "Latch type 3 (opened and closed)" (p. 6-93) shows the open and closed position of the latch. Depending on your pluggable transmission module type, the appearance of the port opening and latch mechanism may vary.

Figure 6-18 Latch type 3 (opened and closed)

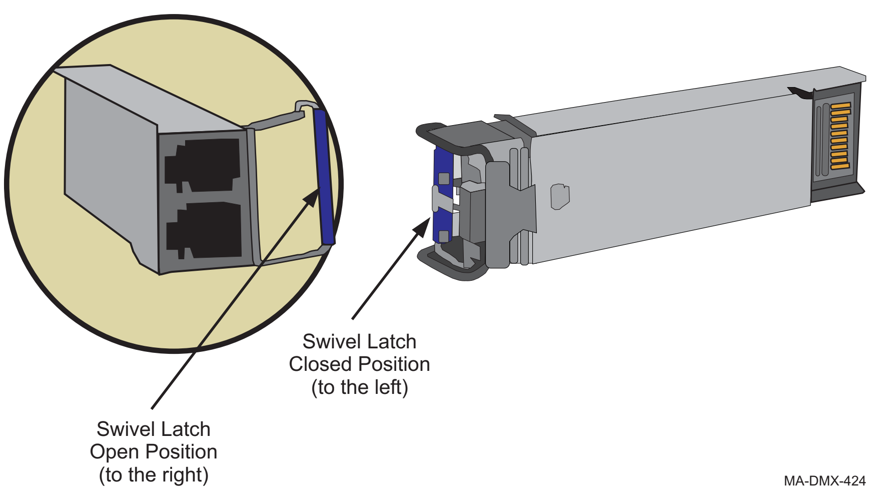


20 Proceed to Step 22.

21 Before inserting the module, the latch must be in the closed position. With the dust cover in place, the latch is in the closed position.

Figure 6-19, "Latch type 4, 5, 6, 7, and 8 (opened and closed)" (p. 6-93) shows the open and closed position of the latch. Depending on your pluggable transmission module type, the appearance of the port opening and latch mechanism may vary.

Figure 6-19 Latch type 4, 5, 6, 7, and 8 (opened and closed)

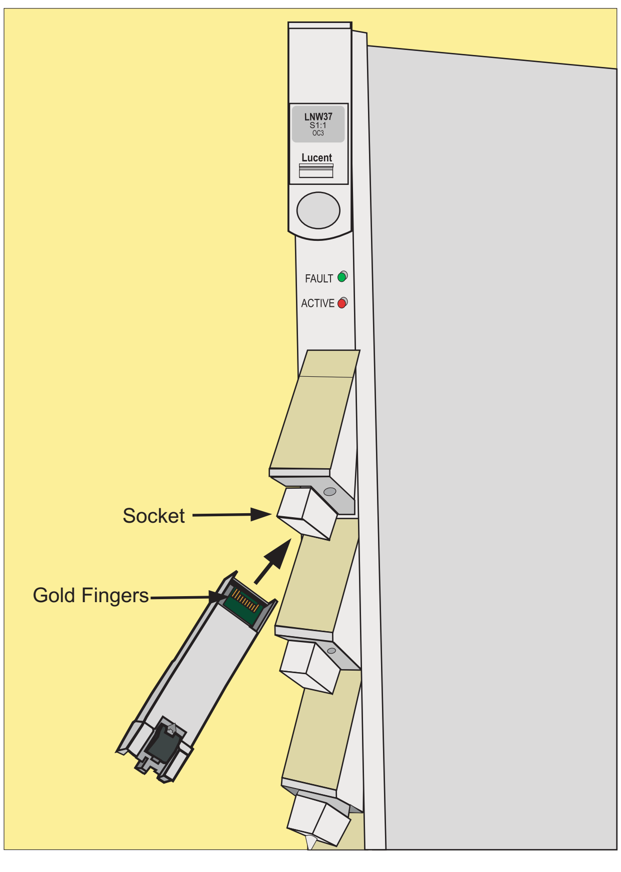


22 With your left hand, hold the pluggable transmission module by the port end or dust cover. The ports are in your left hand and the gold fingers are visible (facing you). (Do not insert pluggable transmission module).

23 Rotate the module; the port end or dust cover is facing you and the gold fingers are facing to the right. (Do not insert pluggable transmission module).

24 Insert the pluggable transmission module in the required socket of the circuit pack faceplate. Confirm that the pluggable transmission module is locked in the socket. Verify that all unused sockets on the circuit pack are equipped with dust covers.

Figure 6-20 Insert pluggable transmission module into socket



Result: The port appears in the *WaveStar*® CIT System View indicating successful installation.

If response is not correct, replace the pluggable transmission module. If the pluggable transmission module fails when inserted, and another pluggable transmission module in the shelf fails at the same time, replace the newly-installed pluggable transmission module. Each pluggable transmission module has unique internal data for warranty purposes. If this data for any reason is not unique, both pluggable transmission modules with the duplicated information will be declared failed.

25 Push on the port end or dust cover to insert the module. The latch automatically catches when the module is inserted. The module is secure.

26 Reconnect the cables.

27

If replacing a pluggable transmission module in an...	Then...
Optical OLIU circuit pack,	Continue with Step 28.
Ethernet or DATA circuit pack,	Proceed to Step 30.

28 If required, clear any Forced 1+1 line protection switch performed in Step 6. Select **Fault** → **Protection Switch**. Click on the required *1+1 Line*, *1+1_optm Line*, or *1+1_bidir Line* protection group and **Select**. Select the *Reset* Switch Type and click **Apply**.

Result: A dialog box appears asking you to confirm executing this command. Click **Yes**.

29 To verify that a 1+1 line switch cleared, perform the following:

1. From the System View menu, select **View** → **Protection**.
2. Highlight the required 1+1, 1+1_optm, or 1+1_bidir line protection group and click **Select**.
3. Verify that Switch Request State is *No Request*.

30 From the System View menu, click the **Alarm List** button to obtain an *NE Alarm List*. Verify that no alarms are present for the installed pluggable transmission module.

If required, refer to the appropriate procedure to clear any alarms.

31 From the System View menu, use **View** → **Equipment** to access the port parameters for the pluggable transmission module just installed and verify that the parameters are intact.

If required, refer to the appropriate procedure in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* to change any parameters.

END OF STEPS

Procedure 6-9: Replace LNW80 switch circuit pack

Overview

Use this procedure to replace an LNW80 Switch circuit packs in Main slots **M1** and **M2**.

The LNW80 Switch circuit pack has *no* optics and is used in headless main applications to allow full use of the VT1.5 switch fabric for VT1.5-type hairpin cross-connections. The LNW80 circuit pack supports equipment-related alarms.

The LNW80 Switch circuit pack requires no provisioning and does not support loopbacks, test access, performance monitoring, DCC functionality, incoming signal alarms, line timing, DS1 synchronization outputs, and upgrades. The LNW80 Switch circuit pack can not be a cross-connection source or destination.

> **Important!** If both the original OLIU circuit pack and the replacement OLIU circuit pack fail when no other transmission circuit packs are installed in the shelf, replace the SYSCTL circuit pack. Refer to Procedure 6-10: “Upgrade or replace SYSCTL (LNW2) circuit pack” (p. 6-99).

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 6-3) and “Required equipment” (p. 6-3) in this chapter.
2. Refer to “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”.
3. Ensure that the correct circuit pack is available for replacement.
4. Obtain the work instructions for this procedure.

Steps

Complete the following steps to replace an LNW80 Switch circuit packs in Main slots **M1** and **M2**.

1 Remove the circuit pack by grasping the inner edge of the locking-levers, and applying a constant pressure, pull the levers forward and remove the circuit pack.

2 Seat the replacement circuit pack in the vacated M1 or M2 slot.

Result: The **FAULT** LED and **ACTIVE** LED lights. The **FAULT** LED flashes after about 20 seconds and then goes off. MJ or MN and NE alarm LEDs on the SYSCTL circuit pack light when the circuit pack is installed.

3 From the System View menu, click the **Alarm List** button to obtain an *NE Alarm List*. Verify that no alarms are present for the installed circuit pack.

If required, refer to the appropriate procedure to clear any alarms.

4 From the System View menu, select **View** → **Equipment** and verify that the new circuit pack is recognized by the SYSCTL.

END OF STEPS

Procedure 6-10: Upgrade or replace SYSCTL (LNW2) circuit pack

Overview

Use this procedure to upgrade/replace a SYSCTL (LNW2) circuit pack in an in-service shelf.

If you wish to upgrade an LNW1 to an LNW2, you must use either Procedure 6-19: “Upgrade software generic via FTAM” (p. 6-218) or Procedure 6-17: “Upgrade software generic via FTP” (p. 6-175).

Important! Performing this procedure under the following scenarios may cause transmission losses and/or require a restore from a remote backup file.

- While the SYSCTL is removed, DO NOT remove or replace either Main circuit pack (M1, M2).
- If an equipped Main (M1 or M2) is removed from the NE, DO NOT replace the SYSCTL.

Required equipment

The following equipment is required:

- At least one of the following cables:
  - RS-232 cable with an RJ-45 connector on one end and a PC serial connector on the other (typically DB9) for the **RS232** port
  - CAT5 Ethernet cable with either a 10/100 hub or a cross-over cable for the front **LAN** or **J16 IAO LAN** ports
- Personal computer (PC) with *WaveStar*® CIT software installed
- Wrist strap

NOTICE

Service-disruption hazard

Failure to equip the expected circuit packs in the shelf and clear any circuit pack-related alarms before replacing the SYSCTL circuit pack can result in a loss of transmission. If this occurs, you can recover transmission by equipping the expected circuit packs and restoring the database.

Equip an expected circuit pack in every slot for which there is an expected circuit pack type.

If the network element is reporting any `CP removed`*,* `CP not allowed`*, or* `Unexpected CP type` *alarms, do* NOT *replace the SYSCTL circuit pack.*

Before you begin

Prior to performing this procedure:

1. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
2. Ensure that a SYSCTL circuit pack is available for replacement.
3. Restoring the network element database may be service-affecting. If provisioning changes were made after the last backup files were created, examine the security log and use the appropriate *WaveStar*® CIT commands to manually apply the recent provisioning changes to the just-restored database.

   Important! If you wish to upgrade an LNW1 to an LNW2, you must use either Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218) or Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175).

Steps

Complete the following steps to replace an LNW2 SYSCTL with an LNW2 SYSCTL.

1 Do you wish to use the upgrade/replace your LNW2 SYSCTL by replacing NVMs or by using Maintenance Mode Wizard (FTP or FTAM)?

If...	Then...
NVM replacement (recommended method)	You must have physical access to your shelf and controller. Your LNW2 may be functioning or failed. Proceed to Procedure 6-10.1: "Upgrade or replace SYSCTL (LNW2) by replacing NVMs" (p. 6-103).
FTAM	Continue with Step 2. Your LNW2 must be functioning; not failed.
FTP	Continue with Step 2. Your LNW2 must be functioning; not failed.

2 Connect the cross-over LAN cable from the Network Interface Card (NIC) on the PC to the front **LAN** port on the SYSCTL circuit pack faceplate and establish a *WaveStar*® CIT session. (When TCP/IP is enabled on the rear LAN port **J16 IAO LAN**, OSI is disabled.)

Start the *WaveStar*® CIT software on the PC by double-clicking on the *WaveStar*® CIT icon on your desktop and login (if necessary). Refer to Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27).

Result: The *Network View* appears.

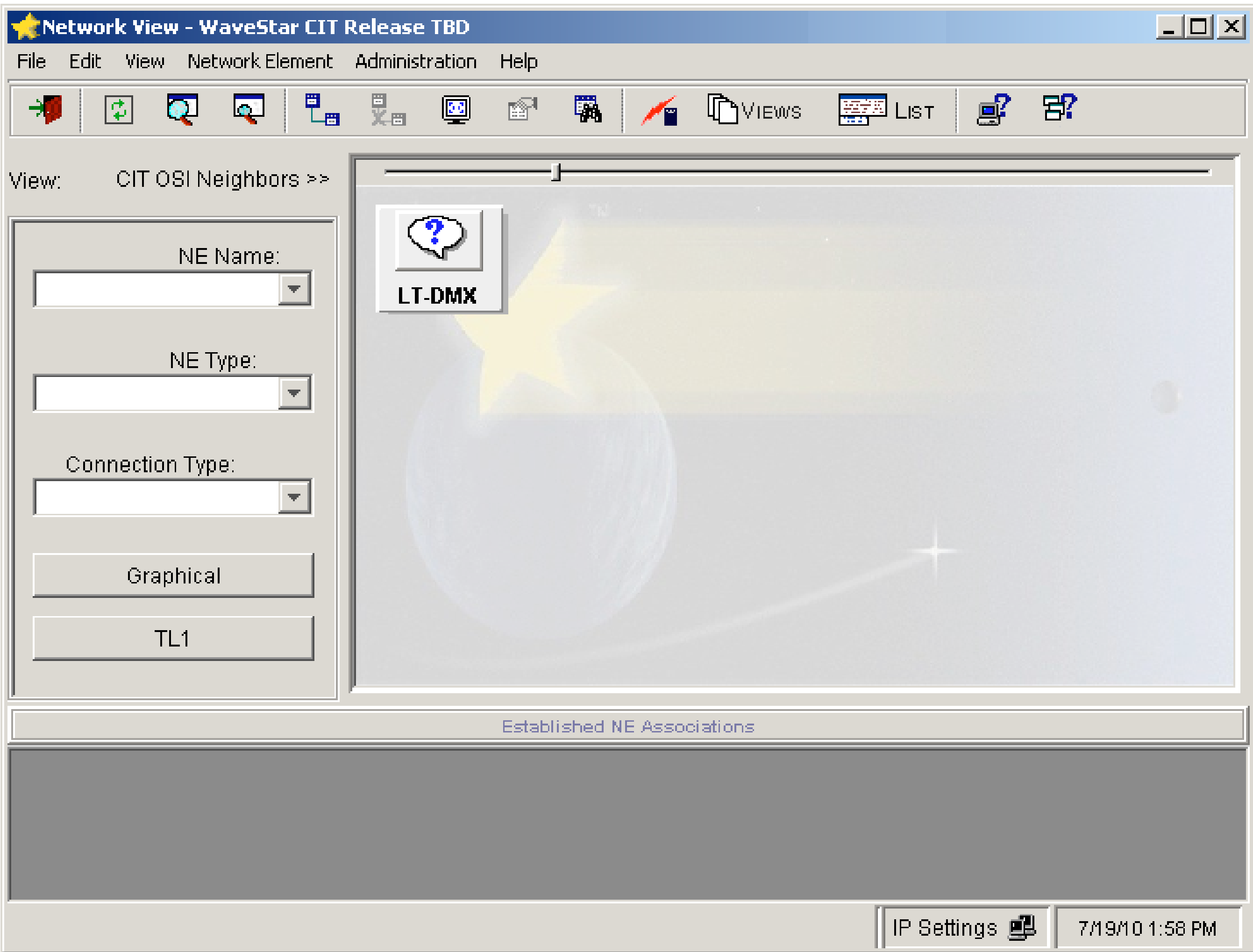
3 From the **View:** pull-down menu, select **CIT OSI Neighbors**.

Important! This **View:** is not the menu bar item View → ...; it is located above the NE Name pull-down menu.

Result: The CIT OSI neighbor(s) are automatically detected.

If you were previously logged in to the NE and/or you do not see your NE, from the Network View, select **View** → **Refresh OSI View**.

Figure 6-21 CIT OSI neighbor



4 In the Network View, right-click the NE icon that was detected (default TID is LT-DMX, your TID may be different), and select **Graphical Using** → **OSI** from the resulting menu.

Result: The *System Type Selection* window appears.

5 In the *System Type Selection* window, select DMX and click **OK**.

Result: The *NE Login Dialog* window appears.

6 In the NE login window, login to the shelf using your user ID and password.

Click **OK**.

7 Would you prefer to use FTAM or FTP to continue with the SYSCTL replacement?

If...	Then...
FTAM	You must have OSI connectivity (via your OSI LAN or DCC) to your shelf. Proceed to Procedure 6-10.2: "Upgrade or replace SYSCTL (LNW2) circuit pack using FTAM" (p. 6-105).
FTP	You must have direct TCP/IP connectivity to your NE and the NE must have a defined IP address. Proceed to Procedure 6-10.3: "Upgrade or replace SYSCTL (LNW2) circuit pack using FTP" (p. 6-126).

END OF STEPS

Procedure 6-10.1: Upgrade or replace SYSCTL (LNW2) by replacing NVMs

Overview

Use this procedure to replace an LNW2 by replacing NVMs.

Important! You must have physical access to your shelf and controller.

Required equipment

Refer to "Required equipment" (p. 6-99) in Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99) for a list of equipment required to perform this procedure.

Before you begin

Prior to performing this procedure, complete Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99).

Steps

Complete the following steps to replace an LNW2 by replacing NVMs.

1 Initiate a ten-second countdown (9, 8, 7, 6, 5, 4, 3, 2, 1, 0) in the **IND** display on the LNW2 SYSCTL by simultaneously depressing the **ACO TEST** and **SEL** buttons on the front of the LNW2 SYSCTL.

Important! Removing the LNW2 without initiating the ten-second countdown may result in unexpected and undesirable protection switches, incorrect circuit fault indications, or incoming signal failure alarms. All SYSCTL functions are suspended during the countdown.

2 Remove the LNW2 SYSCTL circuit pack during the 10-second countdown. This LNW2 will be referred to as the "old" SYSCTL throughout this procedure.

Important! While the SYSCTL circuit pack is removed, do *NOT* remove or replace any transmission circuit packs.

3 Physically remove the NVMs from your old LNW2 and set them aside.

4 Remove the NVMs from your new (replacement) LNW2 and set them aside.

5 Insert the NVMs that you removed from the old SYSCTL in Step 3 in the empty NVM sockets in your new (replacement) LNW2.

6 **Important!** For software installation, ensure that two NVMs are present in the LNW2 SYSCTL. You should have installed the NVMs from your old SYSCTL in your new SYSCTL.

Seat the new LNW2 SYSCTL circuit pack equipped with the NVMs from the old SYSCTL and allow a few minutes for the pack to complete initialization.

Result: The LNW2 SYSCTL exhibits the following visible cycles during initialization:

1. The **FAULT** LED lights and remains lighted for approximately 15 seconds. After approximately 15 seconds, a flashing **b** appears in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 60 seconds and then **IND** display is blank.
2. The **FAULT** LED remains lighted for approximately another 20 seconds and then extinguishes.
3. The **ACTIVE** LED lights and remains lighted.
4. A flashing **b** appears again in the **IND** display on the SYSCTL, indicating that a boot is in progress. After approximately 30 seconds, the **CR** LED flashes 10 times and then extinguishes, and the **b** continues flashing for approximately another 30 seconds, and then **IND** display is blank.
5. The **ACTIVE** LED remains lighted and the other LEDs return to their previous states; prior to the replacement.
6. Continue with Step 7.

7 Proceed to Procedure 6-10.4: "Verify proper software generic" (p. 6-149).

END OF STEPS

Procedure 6-10.2: Upgrade or replace SYSCTL (LNW2) circuit pack using FTAM

Overview

Use this procedure to replace an LNW2 using the File Transfer and Access Management (FTAM) protocol.

Important! You must have OSI connectivity (via your OSI LAN or DCC) to the network element to use FTAM.

Required equipment

Refer to "Required equipment" (p. 6-99) in Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99) for a list of equipment required to perform this procedure.

Before you begin

Prior to performing this procedure, complete Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99).

Steps

Complete the following steps to replace your SYSCTL using FTAM.

---

1 From the System View menu, select **Configuration** → **Software** → **Remote Backup**.

---

2 In the pull-down **Backup To/Via:** menu, select **FTAM**.

---

3 In the **Source/Destination Directory Path** field, enter **`\backups\<filename>`**.

You may also click the **Browse** button next to the *Path:* field to browse to any directory on your PC.

Important! The value of the Path field can be either an absolute path or a relative path that is relative to the root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup. If you selected the default installation location for the *WaveStar*® CIT and software generic: **`\generics\DMX\9.1.x\p`**. If necessary, replace 9.1.0 with your current release, for example 9.1.1. The *WaveStar*® CIT automatically populates the FTAM Responder and NSAP fields.

The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is

`C:\Program Files\Alcatel-Lucent\WaveStar CIT\`

If you wish to store your data in a subdirectory, you may enter **`\backups\<subdirectory>\<filename>`** if the subdirectory exists before the command is sent. Directories will not be created by this command, and therefore the command will be denied if any directory in the path does not already exist.

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.

4 Click **OK**.

You will be asked to verify that you wish to backup to the directory that you entered above. Click **Yes** if you typed the path correctly.

Result: The *Progress Indicator* screen appears, indicating that the backup is in progress. When the backup completes, a `Remote Backup successful` screen appears. Click **OK**. The backup file is now stored. If the default path and a subdirectory were used, the file may be found at:

```
C:\Program Files\Alcatel-Lucent/WaveStar CIT\backups\
<subdirectory>\<filename>
```

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.

5 Close your *WaveStar*® CIT session with the NE. From the System View, select **File** → **NE Disconnect** and click **Yes** in the confirmation window.

Result: The *System View* closes.

6 Disconnect the LAN and/or serial cables from the **LAN** and/or **RS232** port(s) on the front of the LNW2 SYSCTL.

7 Initiate a ten-second countdown (9, 8, 7, 6, 5, 4, 3, 2, 1, 0) in the **IND** display on the LNW2 SYSCTL by simultaneously depressing the **ACO TEST** and **SEL** buttons on the front of the LNW2 SYSCTL.

Important! Removing the LNW2 without initiating the ten-second countdown may result in unexpected and undesirable protection switches, incorrect circuit fault indications, or incoming signal failure alarms. All SYSCTL functions are suspended during the countdown.

8 Remove the SYSCTL circuit pack during the 10-second countdown.

Important! While the SYSCTL circuit pack is removed, do *NOT* remove or replace any transmission circuit packs.

9 **Important!** For installation, two NVMs must be present in the LNW2 SYSCTL. If either NVM is missing, an `NVM removed` alarm will be issued. If both NVM holders are empty, after the circuit pack is installed the **IND** displays an alternating **E** and **0** and **1**. Refer to Step 10 for the complete listing of codes.

Seat the new LNW2 SYSCTL circuit pack and allow a few minutes for the pack to complete initialization.

Result: The LNW2 SYSCTL exhibits the following visible cycles during initialization:

1. The **FAULT** LED lights and remains lighted for approximately 90 seconds. After approximately 15 seconds, a flashing **b** appears in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 75 seconds and then **IND** display is blank.
2. The **FAULT** LED remains lighted for approximately another 20 seconds and then extinguishes.
3. The **ACTIVE** LED lights and remains lighted and the **CR** LED flashes 10 times. While the **CR** LED is flashing, the **MJ**, **ABN**, and **NE** LEDs light and remain lighted.

   Because the LNW2 SYSCTL is in Maintenance Mode, an alternating **M** and **P** and **X** (X represents 6, 7, 8, or 9, depending on your Maintenance Mode) and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **Y** (Y represents 0 or 1, depending on your Maintenance Mode) continue to appear in the **IND** display on the SYSCTL.
4. Continue with Step 10.

10 Observe the **IND** display on the LNW2 SYSCTL; the display indicates the state of the SYSCTL.

If...	**Then...**
alternating **M** and **P** and **6** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	6.0 Maintenance Mode. Continue with Step 11.
alternating **M** and **P** and **7** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	7.0 Maintenance Mode. Continue with Step 11.

If...	Then...
alternating **M** and **P** and **7** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **1**	7.1 Maintenance Mode. Continue with Step 11.
alternating **M** and **P** and **8** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	8.0 Maintenance Mode. Continue with Step 11.
alternating **M** and **P** and **9** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	9.0 Maintenance Mode. Continue with Step 11.
alternating **M** and **P** and **9** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **1**	9.1 Maintenance Mode. Continue with Step 11.
alternating **E** and **0** and **0**	LNW2 SYSCTL must be replaced. Find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
alternating **E** and **0** and **1**	No NVMs are detected on the LNW2 SYSCTL. Install two Alcatel-Lucent-supplied NVMs in the LNW2 or find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
alternating **E** and **0** and **2**	NVMs are present but not readable. Check to make sure they are properly seated and repeat this procedure.
alternating **E** and **0** and **3**	Not Supported. Find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
alternating **E** and **1** and **0**	LNW2 SYSCTL will not boot. No compatible generic on the NVMs in the LNW2 SYSCTL. Find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure or contact your next level of support.
Letter **F**	LNW2 SYSCTL faceplate latches are not fully seated. Unseat the LNW2 SYSCTL and repeat this procedure, properly seating the faceplate latch.
alternating **N** and **O** and **x**	"x" indicates that the NVM socket (1 or 2) is empty or the NVM installed is failed. Replace the indicated NVM or find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.

If...	Then...
Letter **U**	LNW2 SYSCTL will not boot due to unexpected or unreadable shelf type. Repair the problem generally caused by bent pins and repeat this procedure.
flashing **b**	Boot in progress.
A red, four-segment square (2 x 2) appears in the **IND** display on the LNW2 SYSCTL.	Acknowledges the **UPD/INIT** button was momentarily pushed. Pushing the **UPD/INIT** button while in Maintenance Mode has no effect.

11 Connect the cross-over LAN cable from the Network Interface Card (NIC) on the PC to the front **LAN** port on the SYSCTL circuit pack faceplate and establish a *WaveStar*® CIT session. (When TCP/IP is enabled on the rear LAN port **J16 IAO LAN**, OSI is disabled.)

12 From the Network View of the *WaveStar*® CIT session you established in Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99), select the **View:** pull-down menu and select **CIT OSI Neighbors**.

Important! This **View:** is not the menu bar item View → ...; it is located above the NE Name pull-down menu.

13 From the Network View, select **View** → **Refresh OSI View**.

Result: The CIT OSI neighbor(s) are automatically detected.

Your TID will be LT-DMX; when in Maintenance Mode, the TID is always default.

14 In the Network View, right-click the LT-DMX NE icon that was detected, and select **Graphical Using** → **OSI** from the resulting menu.

Result: The *System Type Selection* window appears.

15 In the *System Type Selection* window, select DMX and click **OK**.

Result: The *NE Login Dialog* window appears.

16 **Important!** Because the shelf is in Maintenance Mode, your logins and passwords are default.

Enter the following in the *NE Login Dialog* window (login information is case sensitive) to log in to the NE:

User ID: ***LUC01***

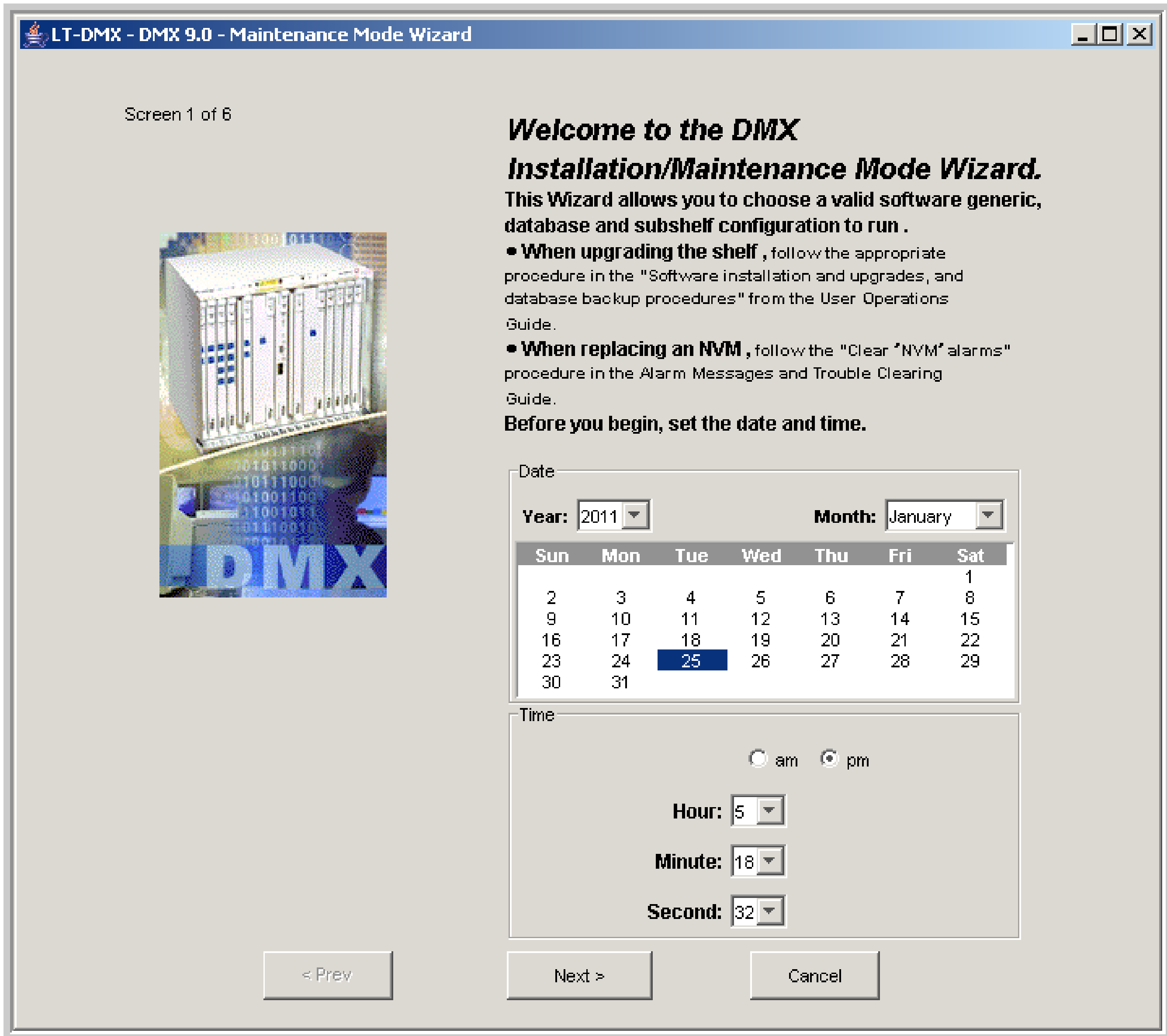
Password: ***DMX2.5G10G***

Click **OK**.

Important! After you select your backup database, complete the Maintenance Mode Wizard, and the NE restarts, your original User IDs and Passwords will be restored.

Result: Screen 1 of 6 in the Maintenance Mode Wizard appears.

Depending on the boot code of your SYSCTL (refer to Step 10), the title bar of the Maintenance Mode Wizard displays either DMX 6.0, DMX 7.0, DMX 7.1, DMX 8.0, DMX 9.0, or DMX 9.1.



This screen picks up the time format preference from the *WaveStar*® CIT.

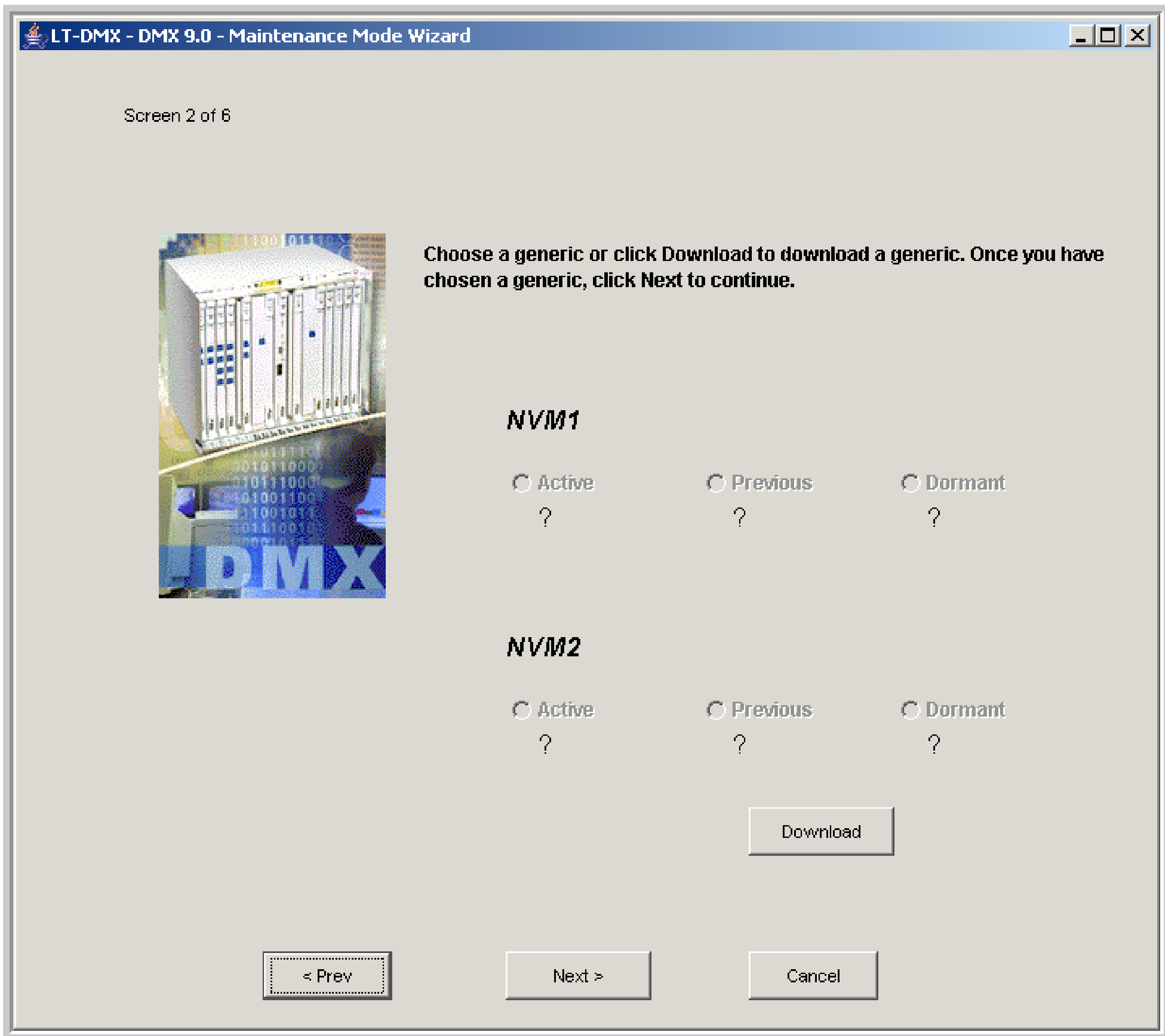
You can provision the time format display for your *WaveStar*® CIT from the Network View by selecting **View** → **Preferences** and clicking on the Display tab. This screen allows you to choose your preference for time format, either a 12-hour clock or a 24-hour clock.

- If your time format preference is a 12-hour clock, from the **Time** panel, select **Hour:** (0–12), **Minute:** (0–59), and **Second:** (0–59) from the pull-down menus. You must also specify am or pm by selecting one of the radio buttons.
- If your time format preference is a 24-hour clock, From the **Time** panel, select the **Hour:** (0–23), **Minute:** (0–59), and **Second:** (0–59) from the pull-down menus.

17 **Important!** The actual time and date are preset from your PC.

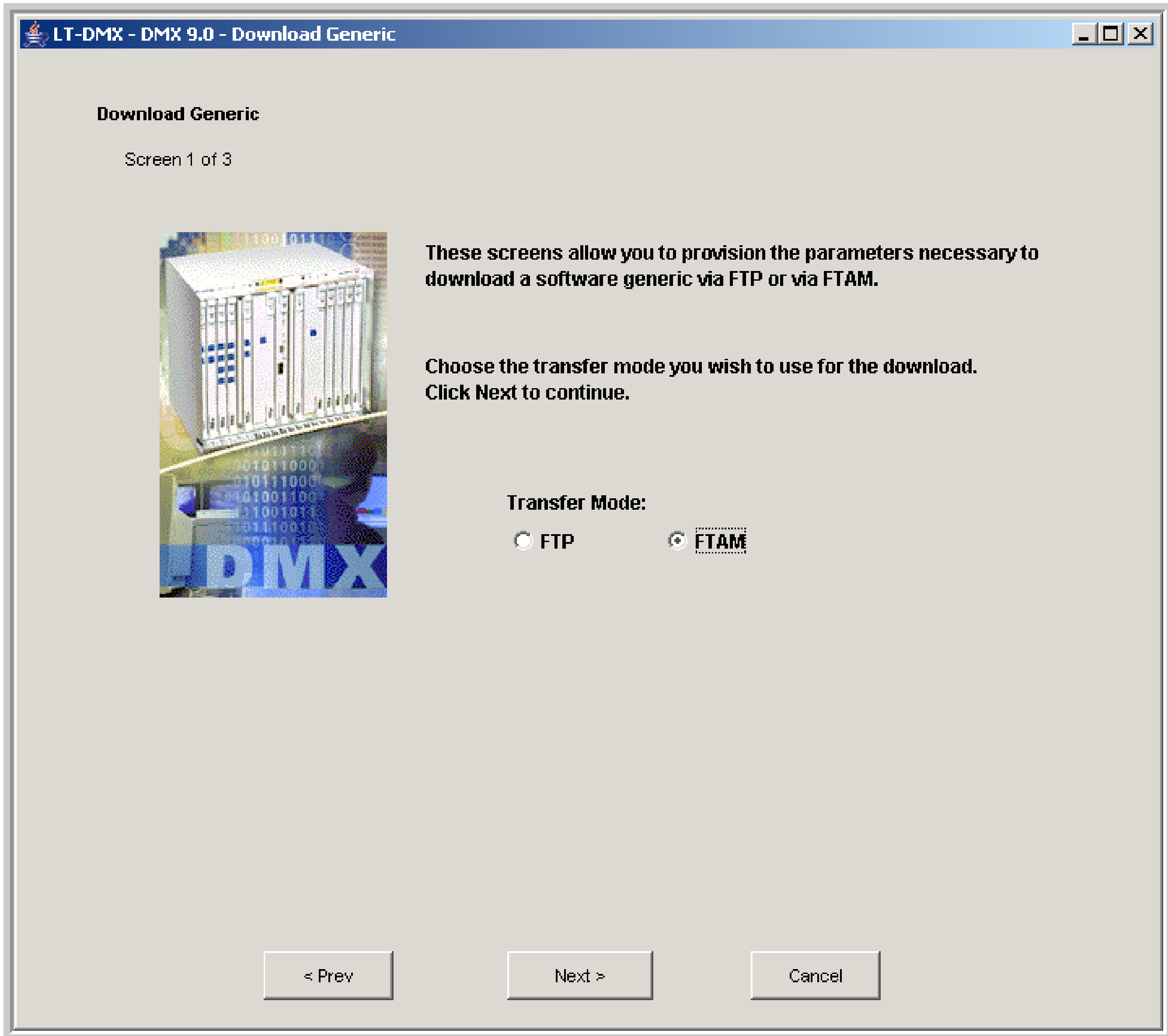
On Screen 1 of 6 in the Maintenance Mode Wizard, read the information, verify the date and time, make any required changes, and click **Next**.

Result: Screen 2 of 6 in the Maintenance Mode Wizard appears.



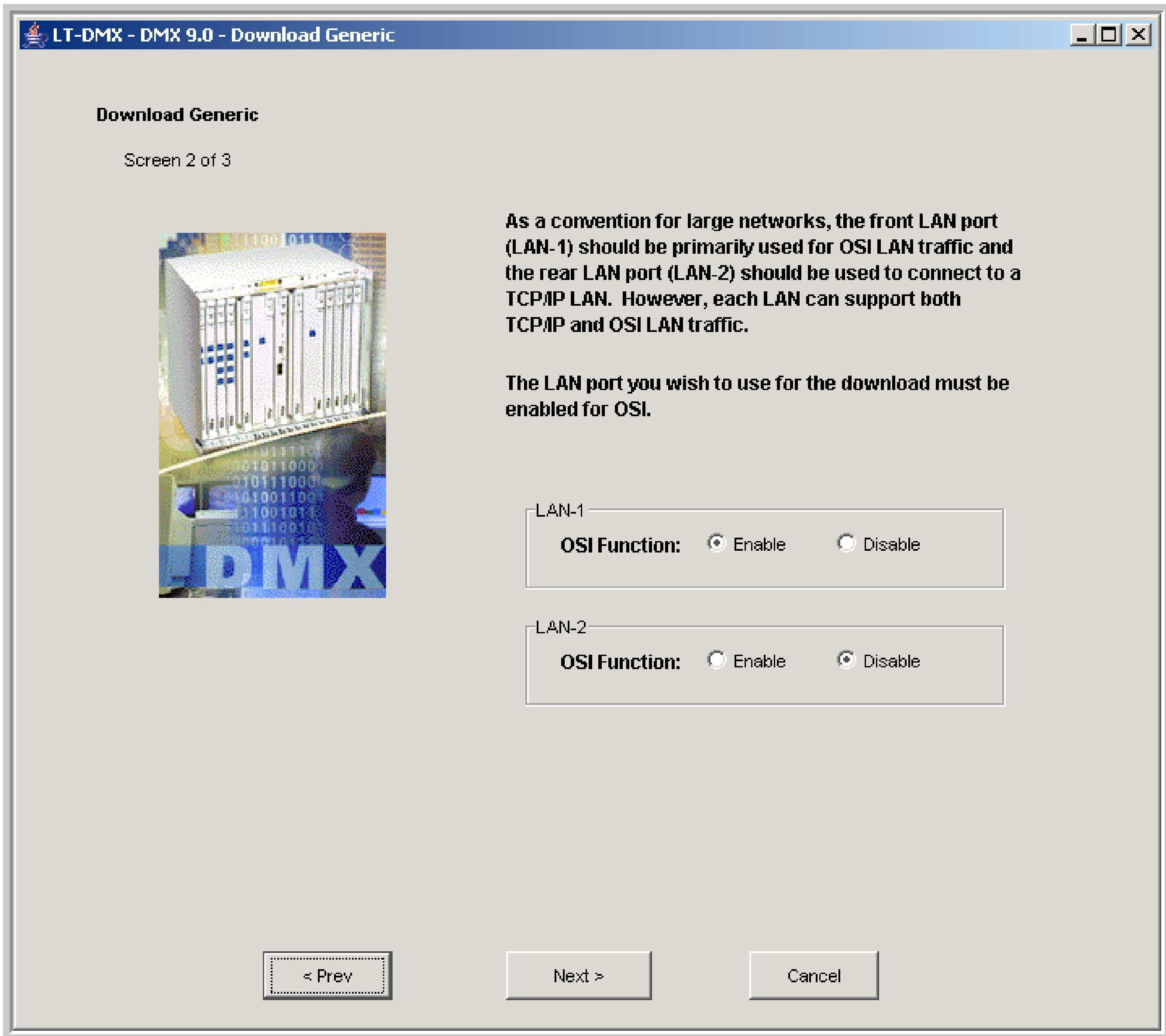
18 On Screen 2 of 6 in the Maintenance Mode Wizard, click **Download**.

Result: Screen 1 of 3 in the Download Generic Wizard appears.



19 On Screen 1 of 3 in the Download Generic Wizard, read the information, select **FTAM** and click **Next**.

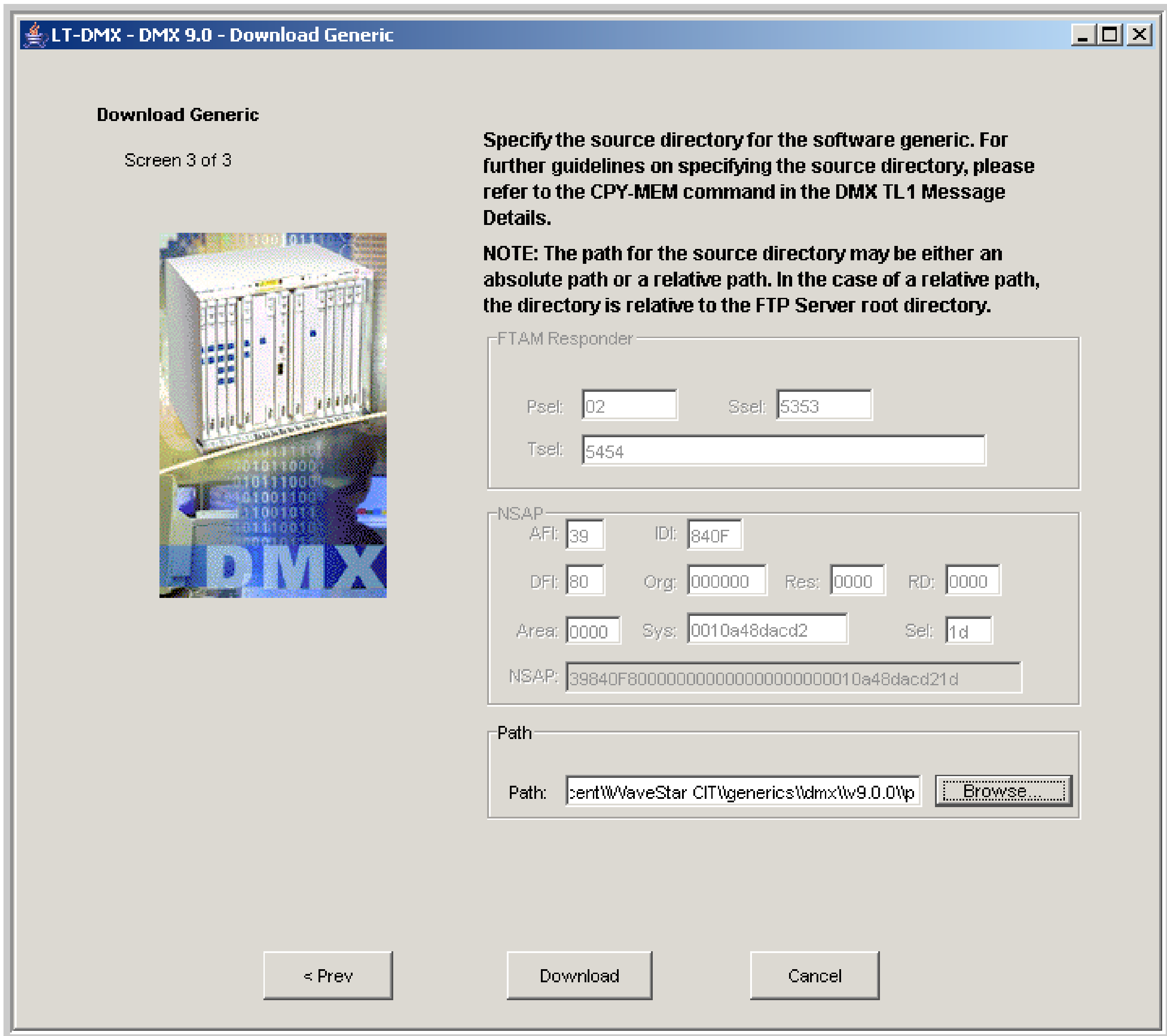
Result: Screen 2 of 3 in the Download Generic Wizard appears.



20 **Important!** LAN-1 is the **LAN** port on the faceplate of the LNW2 SYSCTL circuit pack. LAN-2 is the **J16 IAO LAN** port on the rear of the Alcatel-Lucent 1665 DMX shelf.

On Screen 2 of 3 in the Download Generic Wizard, read the information, verify that the LAN port you are connected to has OSI Function Enable selected and click **Next**.

Result: Screen 3 of 3 in the Download Generic Wizard appears.



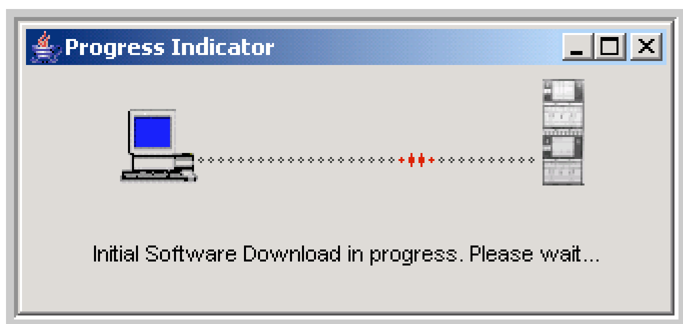
21 On Screen 3 of 3 in the Download Generic Wizard in the **Path** panel, enter the current location of the generic to be downloaded in the Path field or use the **Browse** button to select the generic to be downloaded. Click **Download**.

The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: **`C:\Program Files\Alcatel-Lucent\WaveStar CIT\generics\DMX\9.1.x\p`**. The syntax of the relative path must start with the path name; for example: **`\generics\DMX\9.1.x\p`**. If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\. If necessary, replace 9.1.0 with your current release, for example 9.1.1.

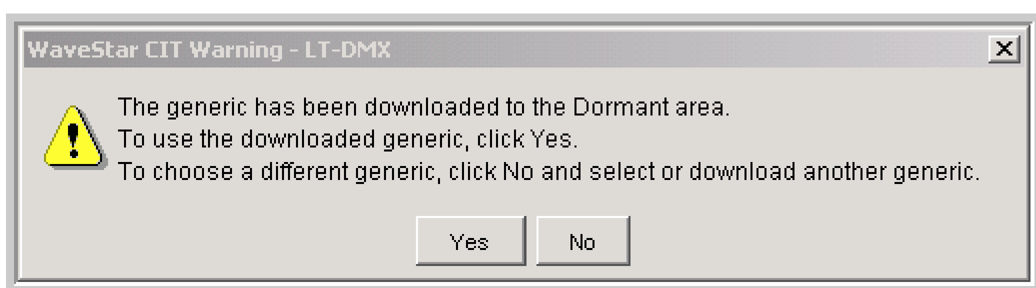
Result: A warning message appears listing the options you provisioned in the previous screens.

22 Verify the information and either click **Yes** to start the download process or click **No** to return to the download screen and change your selections.

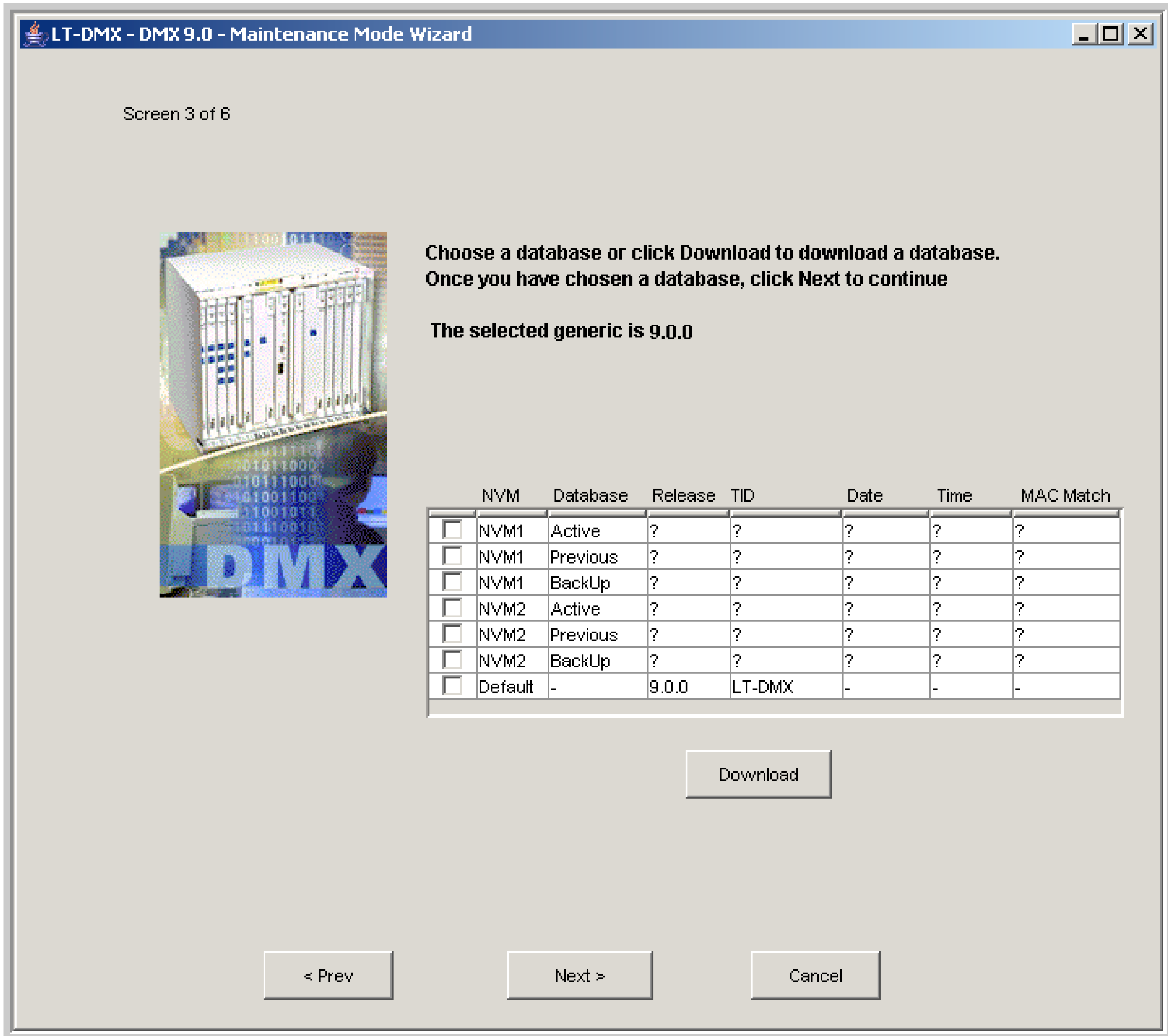
Result: If you choose yes, the following initial software download progress indicator runs for approximately 30 minutes.



23 Once the software generic download is complete, the following confirmation message appears. Click **Yes** to use the generic that is now in the Dormant area.



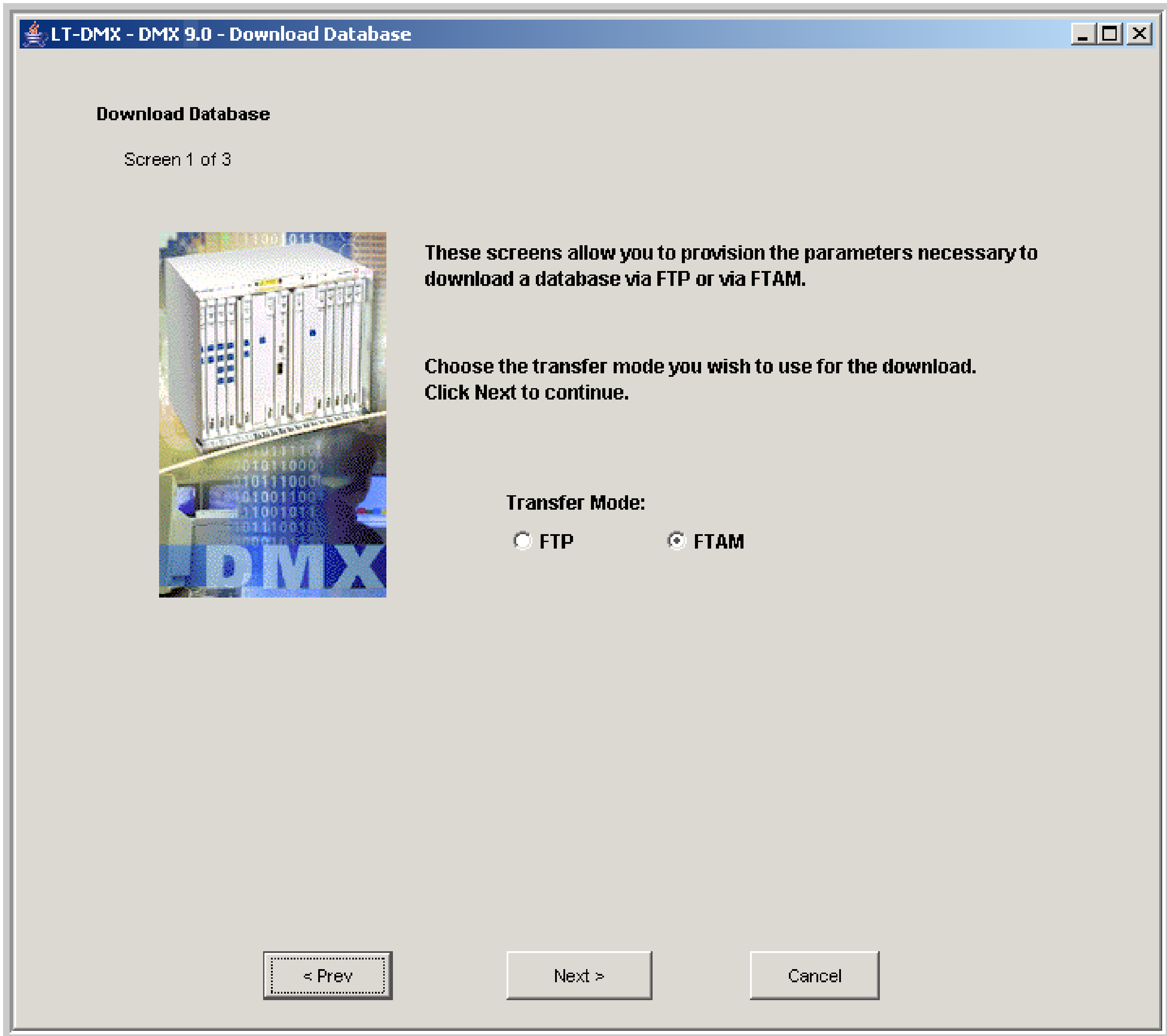
Result: Screen 3 of 6 in the Maintenance Mode Wizard appears.



24 **Important!** Do NOT select the default database or you could loose service to your shelf. You MUST download your previously backed up database.

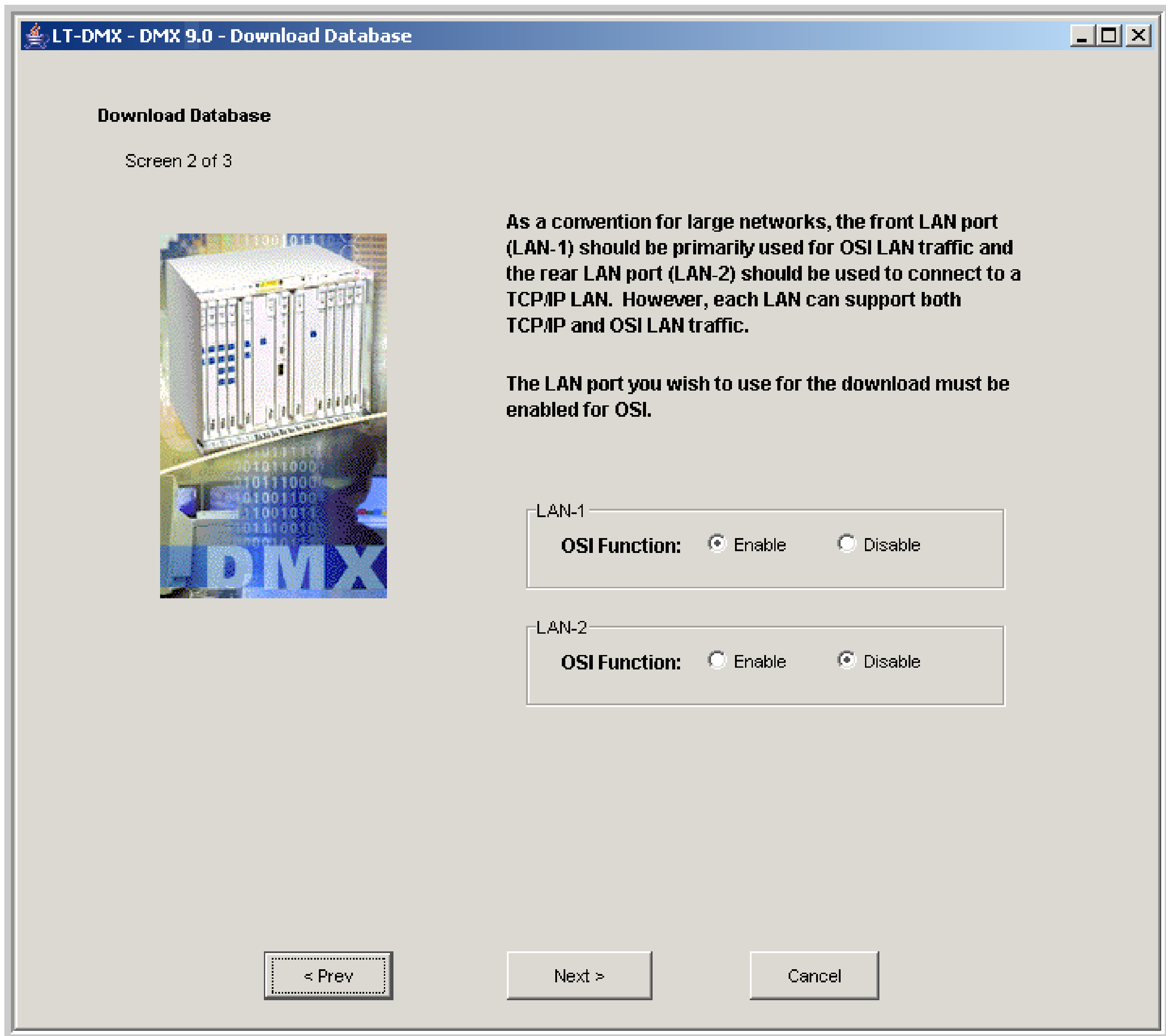
On Screen 3 of 6 in the Maintenance Mode Wizard, click **Download** to select the database you backed up from your original SYSCTL.

Result: Screen 1 of 3 in the Download Database Wizard appears.



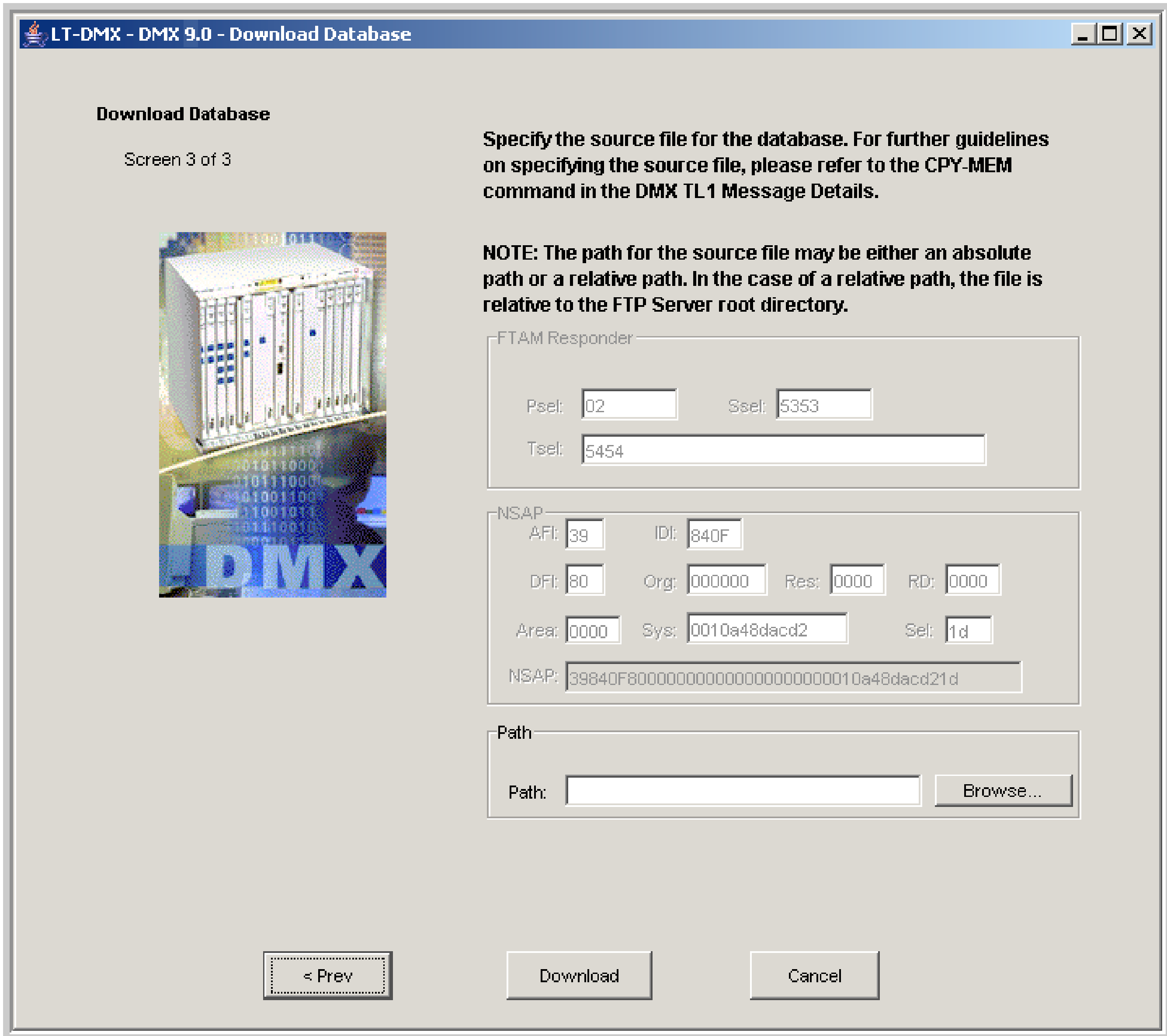
25 On Screen 1 of 3 in the Download Database Wizard, read the information, select **FTAM** and click **Next**.

Result: Screen 2 of 3 in the Download Database Wizard appears.



26 On Screen 2 of 3 in the Download Database Wizard, read the information, verify that the LAN port you are connected to has OSI Function Enable selected and click **Next**.

Result: Screen 3 of 3 in the Download Database Wizard appears.



27 On Screen 3 of 3 in the Download Database Wizard in the **Path** panel, enter the location where the database information is stored. Enter the path and filename exactly as it was entered in Step 3. For example: **\backups\<subdirectory>\<filename>**.

You may also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and select the required file.

Click **Download**.

Important! The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.

The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is

`C:/Program Files/Alcatel-Lucent/WaveStar CIT/`

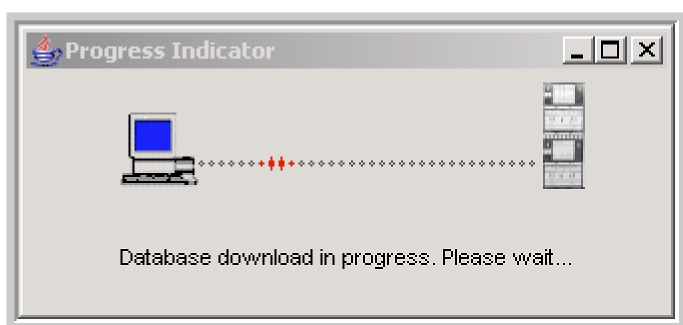
If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.

Result: A warning message appears listing the options you provisioned in the previous screens.

---

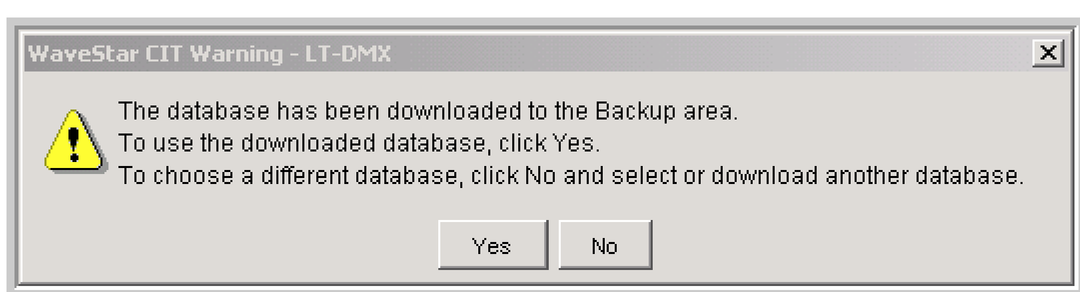
28 Verify the information and click **Yes**.

Result: If you choose Yes, the database download progress indicator runs for approximately two minutes.

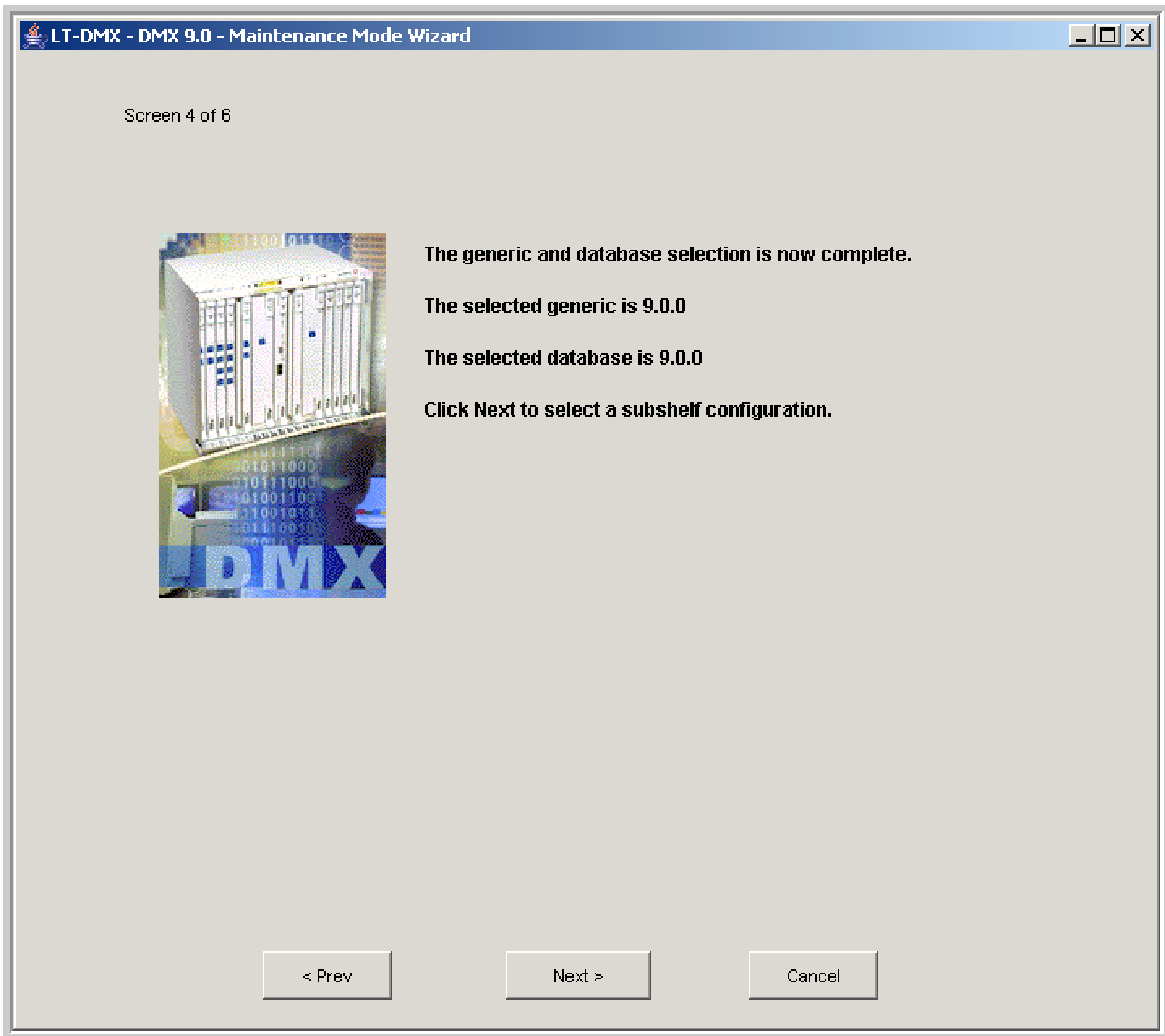


---

29 Once the database download is complete, the following confirmation message appears. Click **Yes** to use the database that is now in the Backup area.

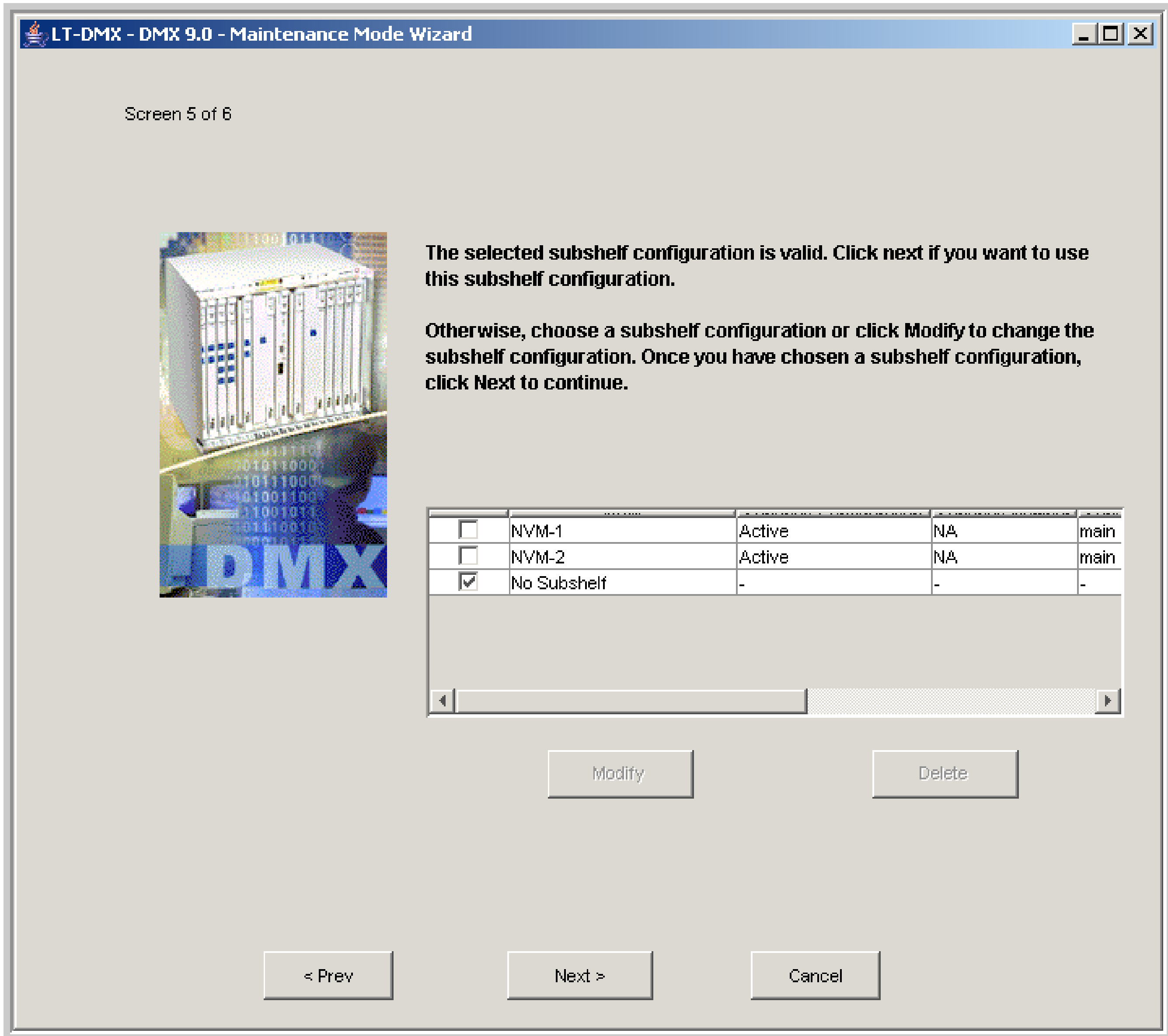


Result: Screen 4 of 6 in the Maintenance Mode Wizard appears. In this screen, 9.1.0 is an example; your selected generic could be different, for example 9.1.1.



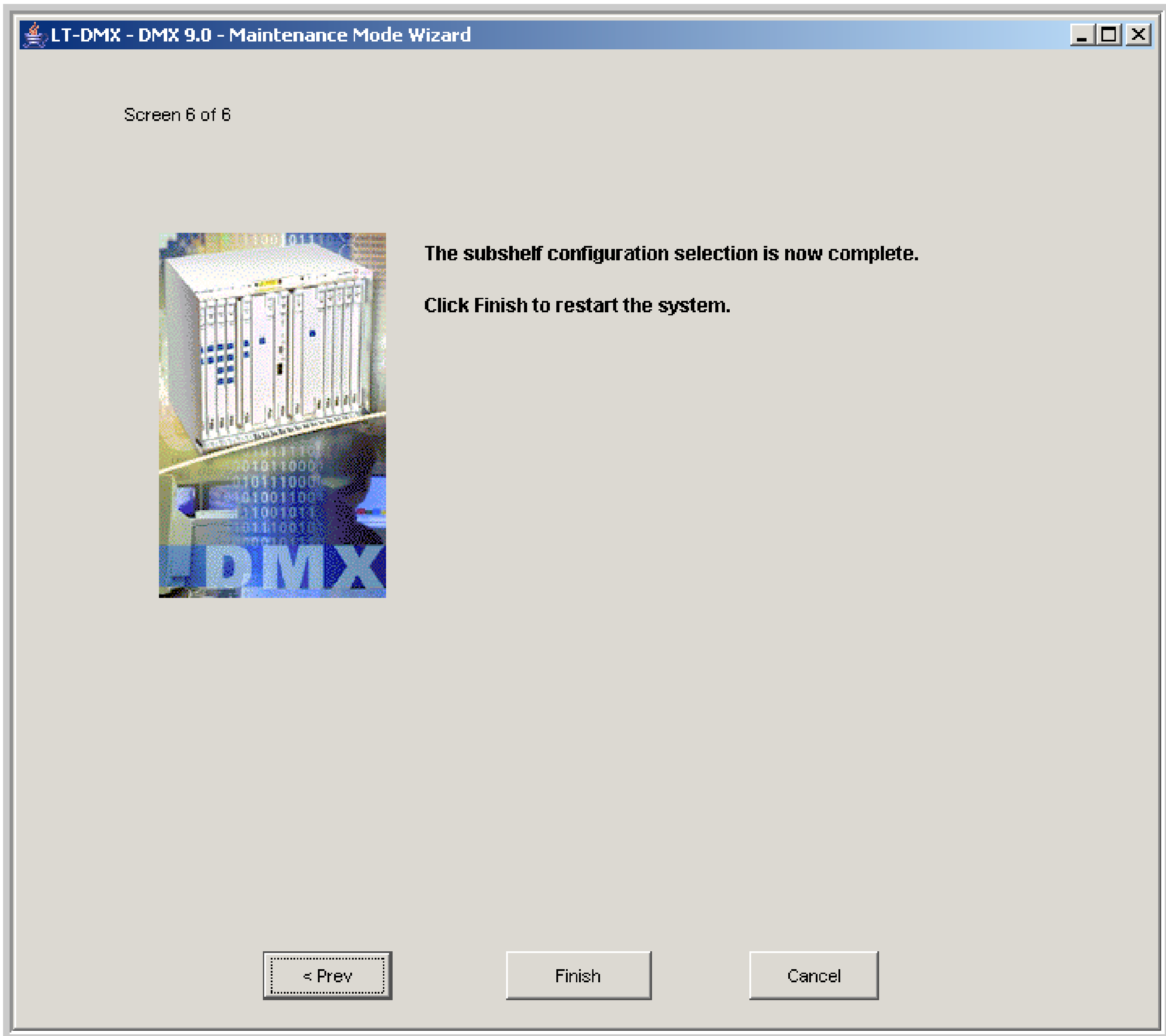
30 On Screen 4 of 6 in the Maintenance Mode Wizard, read the information, verify that you have selected the correct 9.1.x generic and the default database, and click **Next** .

Result: Screen 5 of 6 in the Maintenance Mode Wizard appears.



31 On Screen 5 of 6 in the Maintenance Mode Wizard, select *No Subshelf* or select NVM 1 or 2 if this shelf will be a subshelf and click **Next** .

Result: Screen 6 of 6 in the Maintenance Mode Wizard appears.



32 On Screen 6 of 6 in the Maintenance Mode Wizard, read the information, verify that you have selected the correct generic and database and click **Finish** to restart the system and apply the generic and database.

Result: The Maintenance Mode Wizard closes and your connection to the shelf is terminated.

The LNW2 SYSCTL exhibits the following visible cycles while the generic and database are installed and validated and the SYSCTL reboots:

1. For approximately 20 minutes, the alternating **M** and **P** and **X** (X represents 6, 7, 8, or 9, depending on your Maintenance Mode) and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **Y** (Y represents 0 or 1, depending on your Maintenance Mode) continue to appear in the **IND** display on the SYSCTL.
2. After approximately 20 minutes, all LEDs extinguish and the **IND** display on the SYSCTL is blank for approximately 5 seconds.
3. A flashing **b** appears in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 60 seconds and then **IND** display is blank for approximately 20 seconds.
4. The **ACTIVE** LED lights and remains lighted.
5. A flashing **b** appears again in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 2.5 minutes while the database is being converted and then **IND** display is blank.
6. When nothing appears in the **IND** display and the **ACTIVE** LED is lighted and the other LEDs return to their previous state (pre-backup), the NE software and database installation is complete.

   However, smart circuit packs may be upgrading their firmware. If flashing green **ACTIVE** LEDs are present on a circuit pack, firmware is currently being downloaded to that pack. Wait until all smart circuit packs finish upgrading their firmware before proceeding.

   If an alarm condition existed before the upgrade, the NE rediscovers the alarm condition and activates the appropriate LEDs on the shelf.
7. Continue with Step 33.

---

33 Proceed to Procedure 6-10.4: "Verify proper software generic" (p. 6-149).

END OF STEPS

Procedure 6-10.3: Upgrade or replace SYSCTL (LNW2) circuit pack using FTP

Overview

Use this procedure to replace an LNW2 using File Transfer Protocol (FTP).

Important! You must have direct TCP/IP connectivity to your NE and the NE must have a defined IP address.

Required equipment

Refer to "Required equipment" (p. 6-99) in Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99) for a list of equipment required to perform this procedure.

Before you begin

Prior to performing this procedure, complete Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99).

Steps

Complete the following steps to replace your SYSCTL using FTP.

1 From the System View menu, select **Configuration** → **Software** → **Remote Backup**.

2 In the pull-down **Backup To/Via:** menu, select **FTP**.

3 Select the connection from the **Profile** pull-down menu and proceed to Step 5. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user ID/password may be different.)

4 If you entered connection information in Step 3 and wish to keep the information for future backups:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

   Entries to the **Profile** pull-down menu may be changed using the **Modify**, **Apply**, and **Save** buttons or removed using the **Delete** button.

5 In the **Source/Destination Directory Path** field, enter **`\backups\<filename>`** if you wish to save the backup file to the default location. (If the *WaveStar*® CIT is the FTP server, a maximum of 80 characters is suggested for this field.)

You may also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and over-write the default entry. The **Browse** button is not available (greyed out) if the FTP server is not the local *WaveStar*® CIT.

Important! The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.

The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is

```
C:/Program Files/Alcatel-Lucent/WaveStar CIT/
```

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.

If you wish to store your data in a subdirectory within the default path, you may enter **`\backups\<subdirectory>\<filename>`** if the subdirectory exists before the command is sent. Directories will not be created by this command, and therefore the command will be denied if any directory in the path does not already exist.

6 Click **OK**.

You will be asked to verify that you wish to backup to the directory that you entered above. Click **Yes** if you typed the path correctly.

Result: The *Progress Indicator* screen appears to indicate that the backup is in progress. When the backup completes, a *WaveStar*® CIT information screen appears that indicates `Remote Backup successful`. Click the **OK** button.

The backup file is now stored. If the default path and a subdirectory were used, the file may be found at:

```
C:/Program Files/Alcatel-Lucent/WaveStar CIT/backups/
<subdirectory>/<filename>
```

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.

7 Close your *WaveStar*® CIT session with the NE. From the System View, select **File** → **NE Disconnect** and click **Yes** in the confirmation window.

Result: The *System View* closes.

8 Disconnect the LAN and/or serial cables from the **LAN** and/or **RS232** port(s) on the front of the LNW2 SYSCTL.

9 Initiate a ten-second countdown (9, 8, 7, 6, 5, 4, 3, 2, 1, 0) in the **IND** display on the LNW2 SYSCTL by simultaneously depressing the **ACO TEST** and **SEL** buttons on the front of the LNW2 SYSCTL.

Important! Removing the LNW2 without initiating the ten-second countdown may result in unexpected and undesirable protection switches, incorrect circuit fault indications, or incoming signal failure alarms. All SYSCTL functions are suspended during the countdown.

10 Remove the SYSCTL circuit pack during the 10-second countdown.

Important! While the SYSCTL circuit pack is removed, do *NOT* remove or replace any transmission circuit packs.

11 **Important!** For installation, two NVMs must be present in the LNW2 SYSCTL. If either NVM is missing, an `NVM removed` alarm will be issued. If both NVM holders are empty, after the circuit pack is installed the **IND** displays an alternating **E** and **0** and **1**. Refer to Step 12 for the complete listing of codes.

Seat the new LNW2 SYSCTL circuit pack and allow a few minutes for the pack to complete initialization.

Result: The LNW2 SYSCTL exhibits the following visible cycles during initialization:

1. The **FAULT** LED lights and remains lighted for approximately 90 seconds. After approximately 15 seconds, a flashing **b** appears in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 75 seconds and then **IND** display is blank.
2. The **FAULT** LED remains lighted for approximately another 20 seconds and then extinguishes.
3. The **ACTIVE** LED lights and remains lighted and the **CR** LED flashes 10 times. While the **CR** LED is flashing, the **MJ**, **ABN**, and **NE** LEDs light and remain lighted.

   Because the LNW2 SYSCTL is in Maintenance Mode, an alternating **M** and **P** and **X** (X represents 6, 7, 8, or 9, depending on your Maintenance Mode) and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **Y** (Y represents 0 or 1, depending on your Maintenance Mode) continue to appear in the **IND** display on the SYSCTL.
4. Continue with Step 12.

12 Observe the **IND** display on the LNW2 SYSCTL; the display indicates the state of the SYSCTL.

If...	Then...
alternating **M** and **P** and **6** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	6.0 Maintenance Mode. Continue with Step 13.
alternating **M** and **P** and **7** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	7.0 Maintenance Mode. Continue with Step 13.
alternating **M** and **P** and **7** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **1**	7.1 Maintenance Mode. Continue with Step 13.
alternating **M** and **P** and **8** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	8.0 Maintenance Mode. Continue with Step 13.
alternating **M** and **P** and **9** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	9.0 Maintenance Mode. Continue with Step 13.
alternating **M** and **P** and **9** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **1**	9.1 Maintenance Mode. Continue with Step 13.

If...	**Then...**
alternating **E** and **0** and **0**	LNW2 SYSCTL must be replaced. Find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
alternating **E** and **0** and **1**	No NVMs are detected on the LNW2 SYSCTL. Install two Alcatel-Lucent-supplied NVMs in the LNW2 or find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
alternating **E** and **0** and **2**	NVMs are present but not readable. Check to make sure they are properly seated and repeat this procedure.
alternating **E** and **0** and **3**	Not Supported. Find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
alternating **E** and **1** and **0**	LNW2 SYSCTL will not boot. No compatible generic on the NVMs in the LNW2 SYSCTL. Find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure or contact your next level of support.
Letter **F**	LNW2 SYSCTL faceplate latches are not fully seated. Unseat the LNW2 SYSCTL and repeat this procedure, properly seating the faceplate latch.
alternating **N** and **O** and **x**	"x" indicates that the NVM socket (1 or 2) is empty or the NVM installed is failed. Replace the indicated NVM or find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
Letter **U**	LNW2 SYSCTL will not boot due to unexpected or unreadable shelf type. Repair the problem generally caused by bent pins and repeat this procedure.
flashing **b**	Boot in progress.
A red, four-segment square (2 x 2) appears in the **IND** display on the LNW2 SYSCTL.	Acknowledges the **UPD/INIT** button was momentarily pushed. Pushing the **UPD/INIT** button while in Maintenance Mode has no effect.

13 Connect the cross-over LAN cable from the Network Interface Card (NIC) on the PC to the front **LAN** port on the SYSCTL circuit pack faceplate and establish a *WaveStar*® CIT session. (When TCP/IP is enabled on the rear LAN port **J16 IAO LAN**, OSI is disabled.)

14 From the Network View of the *WaveStar*® CIT session you established in Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99), select the **View:** pull-down menu and select **CIT OSI Neighbors**.

Important! This **View:** is not the menu bar item View → ...; it is located above the NE Name pull-down menu.

Result: The CIT OSI Neighbor(s) are automatically detected.

If you were previously logged in to the NE and/or you do not see your NE, from the Network View, select **View** → **Refresh OSI View**.

15 In the Network View, right-click the LT-DMXtend NE icon that was detected, and select **Graphical Using** → **OSI** from the resulting menu.

Result: The *System Type Selection* window appears.

16 In the *System Type Selection* window, select LT-DMX and click **OK**.

Result: The *NE Login Dialog* window appears.

17 **Important!** Because the shelf is in Maintenance Mode, your logins and passwords are default.

Enter the following in the *NE Login Dialog* window (login information is case sensitive) to log in to the NE:

User ID: ***LUC01***

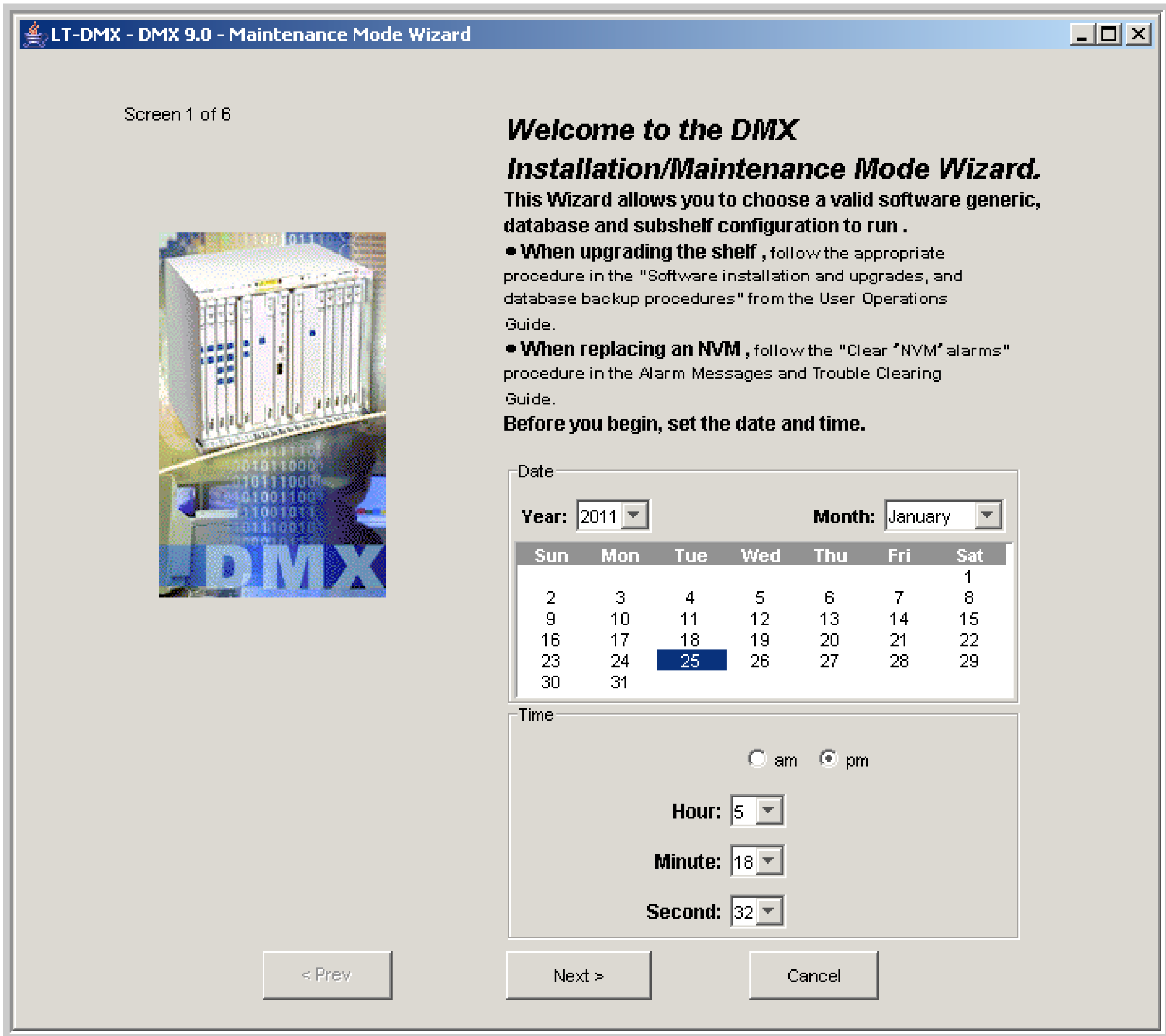
Password: ***DMX2.5G10G***

Click **OK**.

Important! After you select your backup database, complete the Maintenance Mode Wizard, and the NE restarts, your original User IDs and Passwords will be restored.

Result: Screen 1 of 6 in the Maintenance Mode Wizard appears.

Depending on the boot code of your SYSCTL (refer to Step 12), the title bar o f the Maintenance Mode Wizard displays either DMX 6.0, DMX 7.0, DMX 7.1, DMX 8.0, DMX 9.0, or DMX 9.1.



This screen picks up the time format preference from the *WaveStar*® CIT.

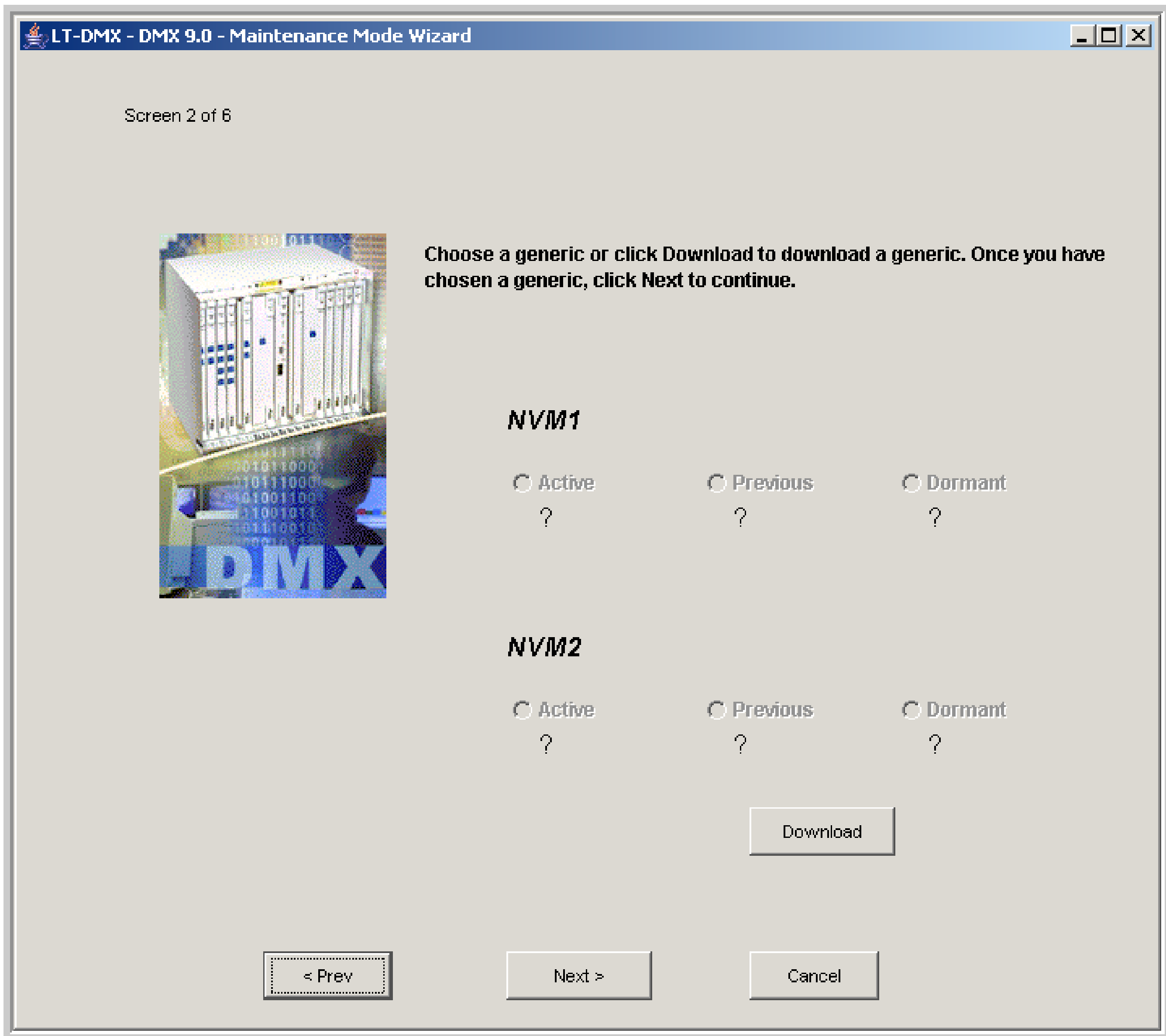
You can provision the time format display for your *WaveStar*® CIT from the Network View by selecting **View** → **Preferences** and clicking on the Display tab. This screen allows you to choose your preference for time format, either a 12-hour clock or a 24-hour clock.

- If your time format preference is a 12-hour clock, from the **Time** panel, select **Hour:** (0–12), **Minute:** (0–59), and **Second:** (0–59) from the pull-down menus. You must also specify am or pm by selecting one of the radio buttons.
- If your time format preference is a 24-hour clock, From the **Time** panel, select the **Hour:** (0–23), **Minute:** (0–59), and **Second:** (0–59) from the pull-down menus.

18 **Important!** The actual time and date are preset from your PC.

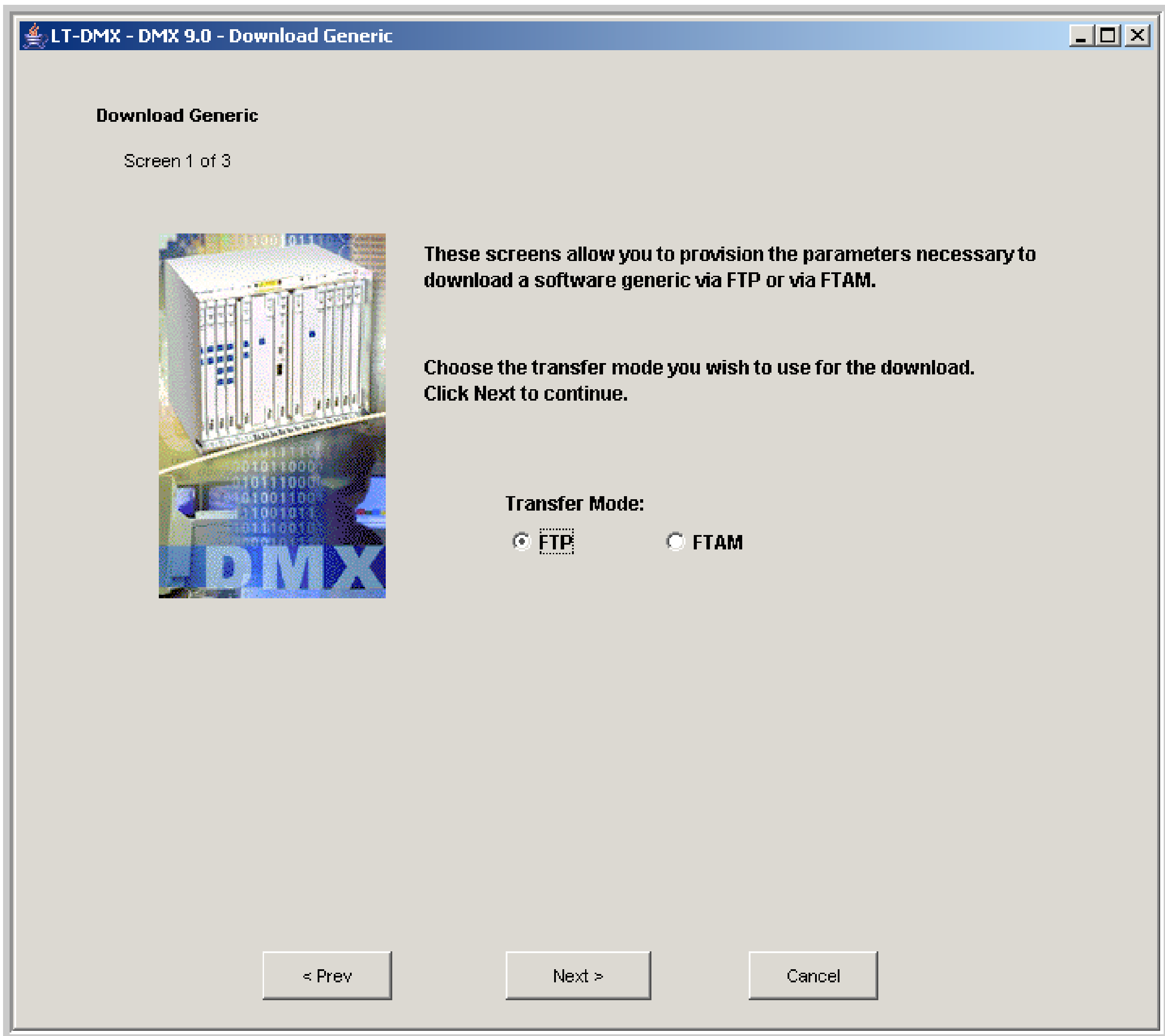
On Screen 1 of 6 in the Maintenance Mode Wizard, read the information, verify the date and time, make any required changes, and click **Next**.

Result: Screen 2 of 6 in the Maintenance Mode Wizard appears.



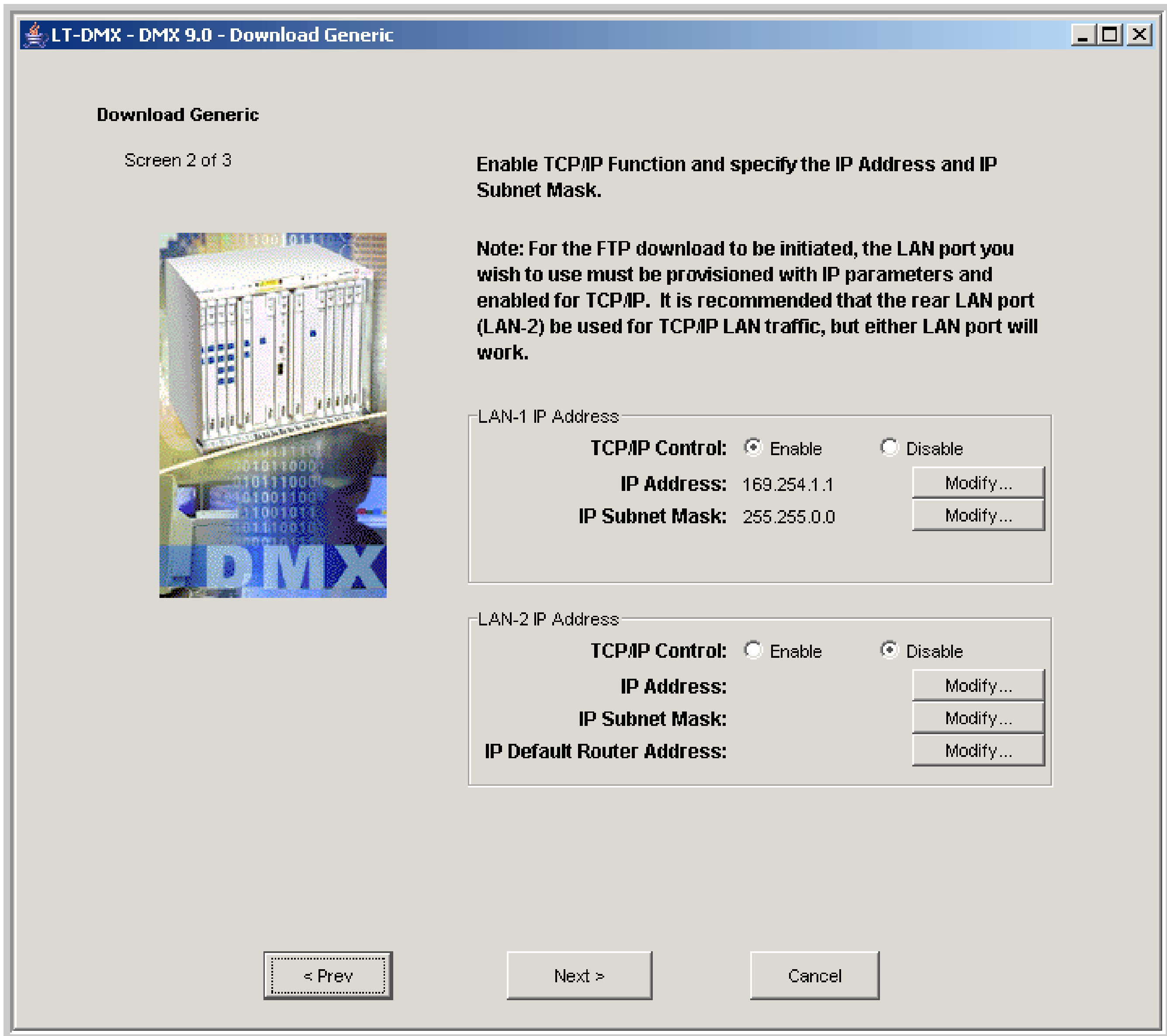
19 On Screen 2 of 6 in the Maintenance Mode Wizard, click **Download**.

Result: Screen 1 of 3 in the Download Generic Wizard appears.



20 On Screen 1 of 3 in the Download Generic Wizard, read the information, select **FTP** and click **Next**.

Result: Screen 2 of 3 in the Download Generic Wizard appears.



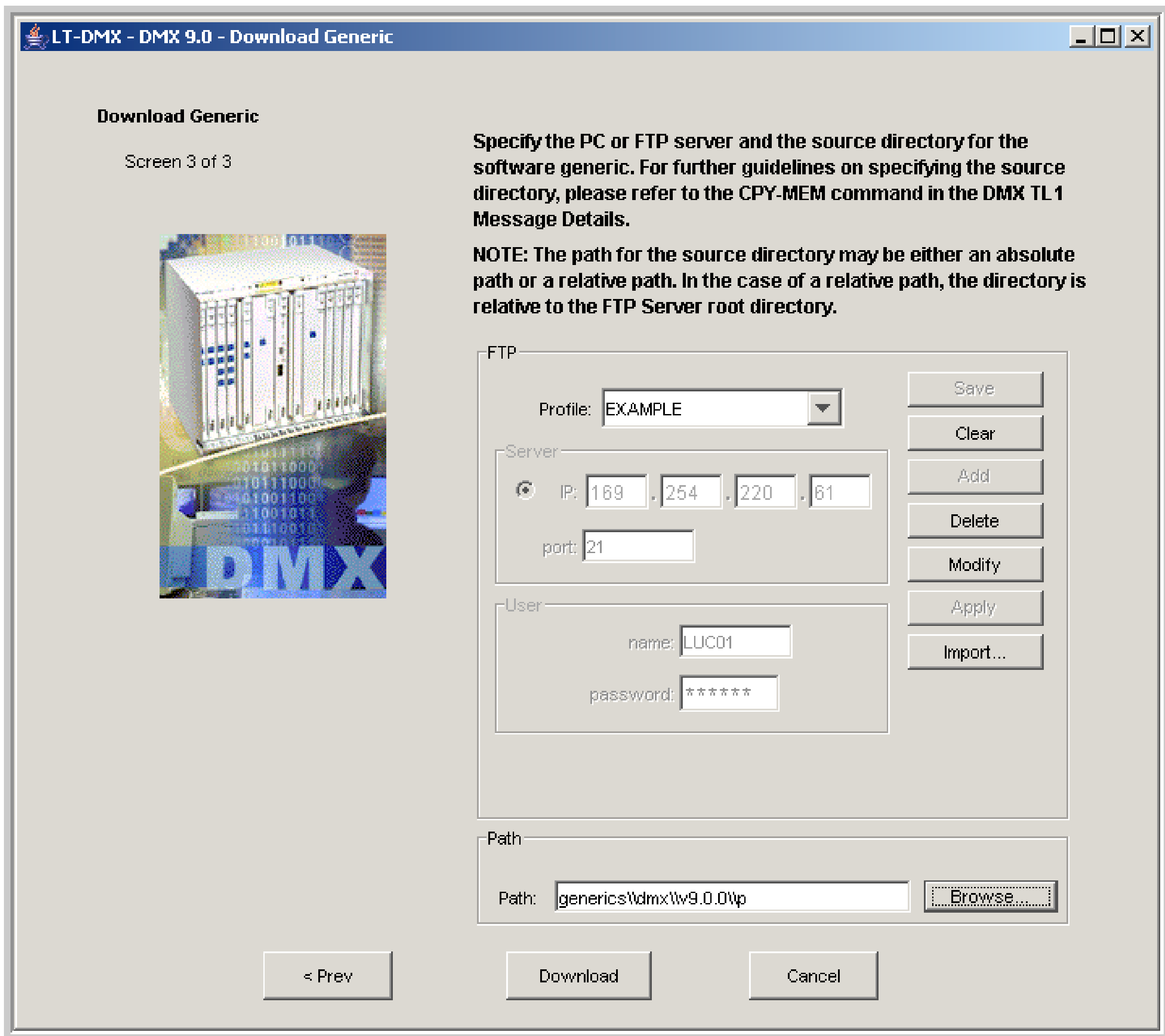
21 **Important!** LAN-1 is the **LAN** port on the faceplate of the LNW2 SYSCTL circuit pack. LAN-2 is the **J16 IAO LAN** port on the rear of the Alcatel-Lucent 1665 DMX shelf.

If the boot code of your LNW2 (Step 12) was 7.1 or later, you may see the IP Address and IP Subnet Mask field populated with the defaults illustrated in Screen 2 of 3.

Important! If the default IP address and subnet mask are present, you must complete the initial software installation before you can change these values.

If required, follow the instructions to enable TCP/IP Control on the LAN port to which you are connected. Click **Modify** to enter the IP Address, IP Subnet Mask, and/or IP Default Router Address. If you are connecting directly to the shelf without a router, the IP address of the FTP server must be in the same subnet as the LAN port. Click **Next**.

Result: Screen 3 of 3 in the Download Generic Wizard appears.



22 Select the connection from the **Profile** pull-down menu and proceed to Step 24. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user ID/password may be different.)

23 If you entered connection information in Step 22 and wish to keep the information for future FTP activities:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

Important! Entries to the **Profile** pull-down menu may be changed using the **Modify**, **Apply**, and **Save** buttons or removed using the **Delete** button.

24 On Screen 3 of 3 in the Download Generic Wizard in the **Path** panel, enter the current location of the generic to be downloaded in the Path field or use the **Browse** button to select the generic to be downloaded. (If the FTP server is not the local host, the **Browse** button is greyed out.) Click **Download**.

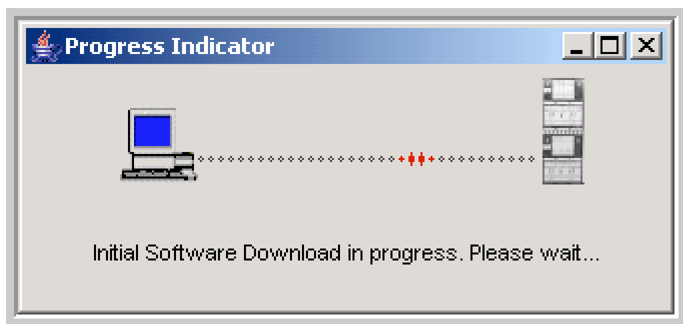
The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: **`C:\Program Files\Alcatel-Lucent\WaveStar CIT\generics\DMX\9.1.x\p`**. The syntax of the relative path must start with the path name; for example: **`\generics\DMX\9.1.x\p`**. If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\. If necessary, replace 9.1.0 with your current release, for example 9.1.1.

If the FTP server is not the *WaveStar*® CIT, then enter the path starting at the FTP home directory on the server.

Result: A warning message appears listing the options you provisioned in the previous screens.

25 Verify the information and either click **Yes** to start the download process or click **No** to return to the download screen and change your selections.

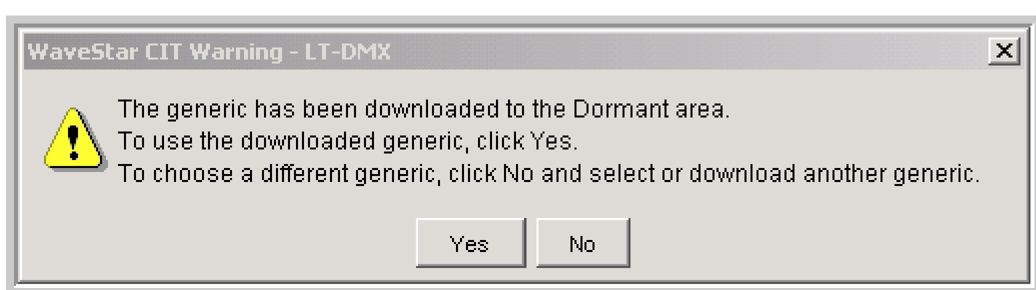
Result: If you choose yes, the following initial software download progress indicator runs for approximately 30 minutes.



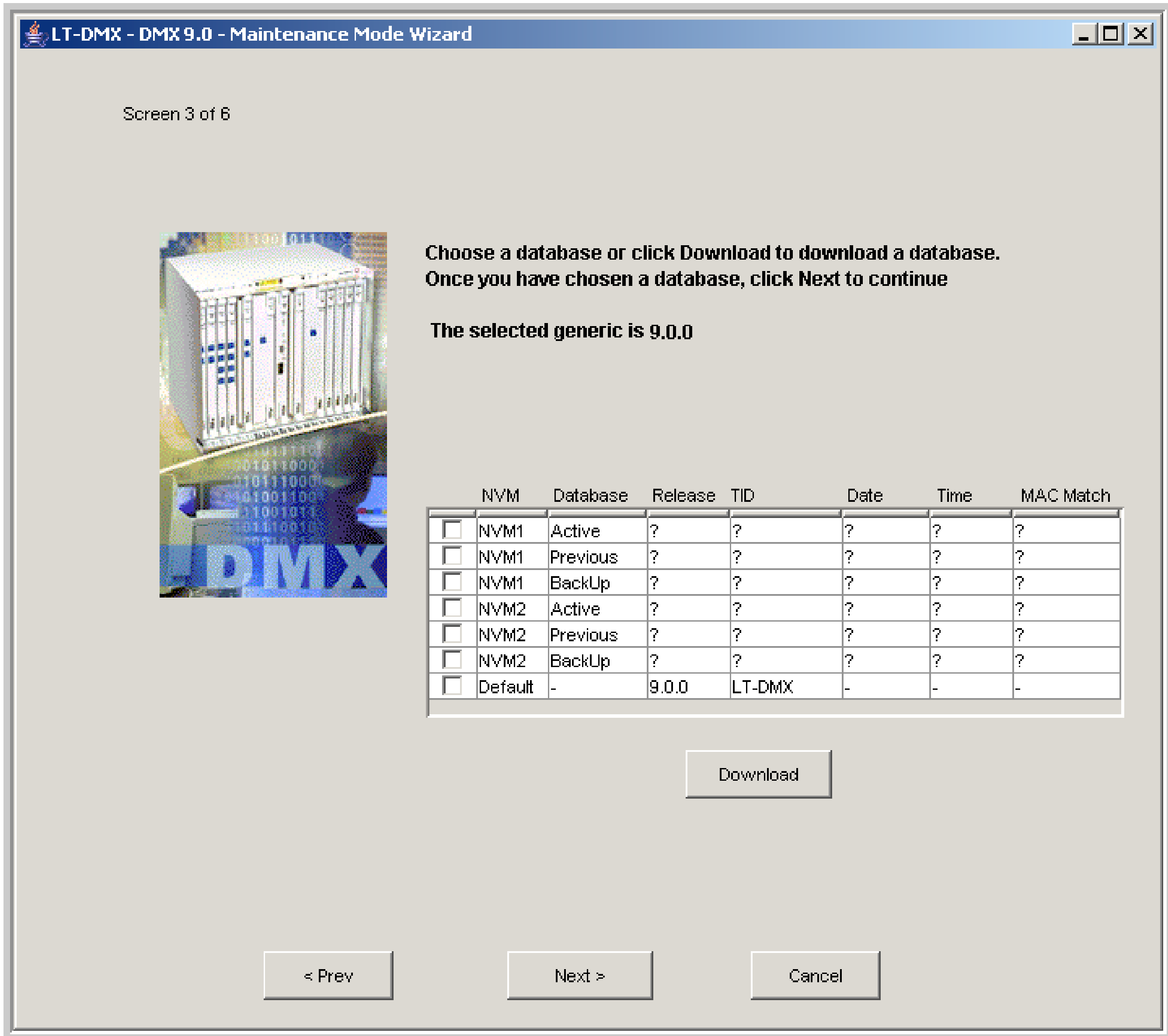
26 Do you wish to observe the FTP download progress?

If...	Then...
Yes	Proceed to Procedure 6-24: "Observe FTP progress" (p. 6-285) and then continue with Step 27.
No	Continue with Step 27.

27 Once the software generic download is complete, the following confirmation message appears. Click **Yes** to use the generic that is now in the Dormant area.



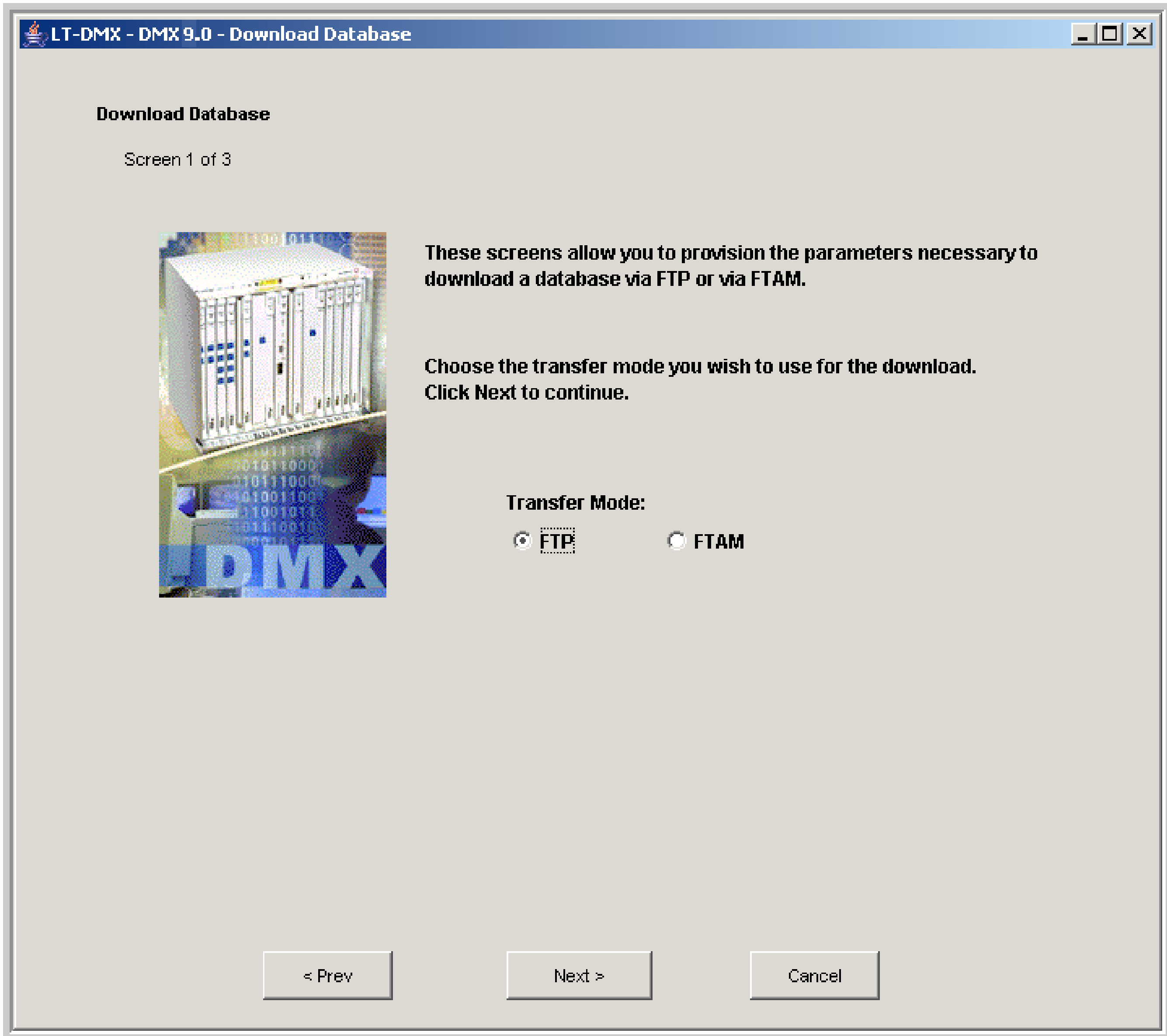
Result: Screen 3 of 6 in the Maintenance Mode Wizard appears.



28 **Important!** Do NOT select the default database or you could loose service to your shelf. You MUST download your previously backed up database.

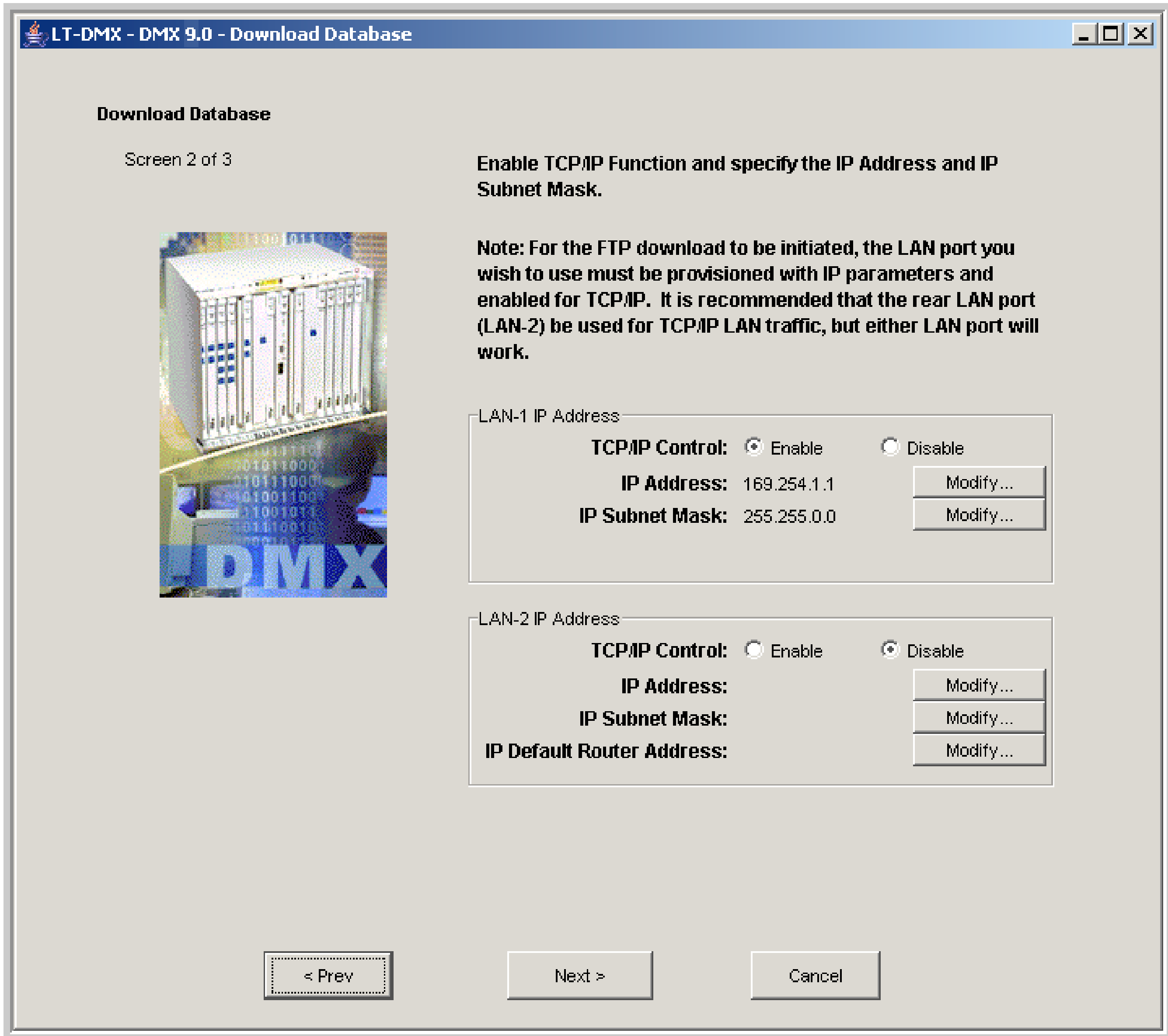
On Screen 3 of 6 in the Maintenance Mode Wizard, click **Download** to select the database you backed up from your original SYSCTL.

Result: Screen 1 of 3 in the Download Database Wizard appears.



29 On Screen 1 of 3 in the Download Database Wizard, read the information, select **FTP** and click **Next**.

Result: Screen 2 of 3 in the Download Database Wizard appears.

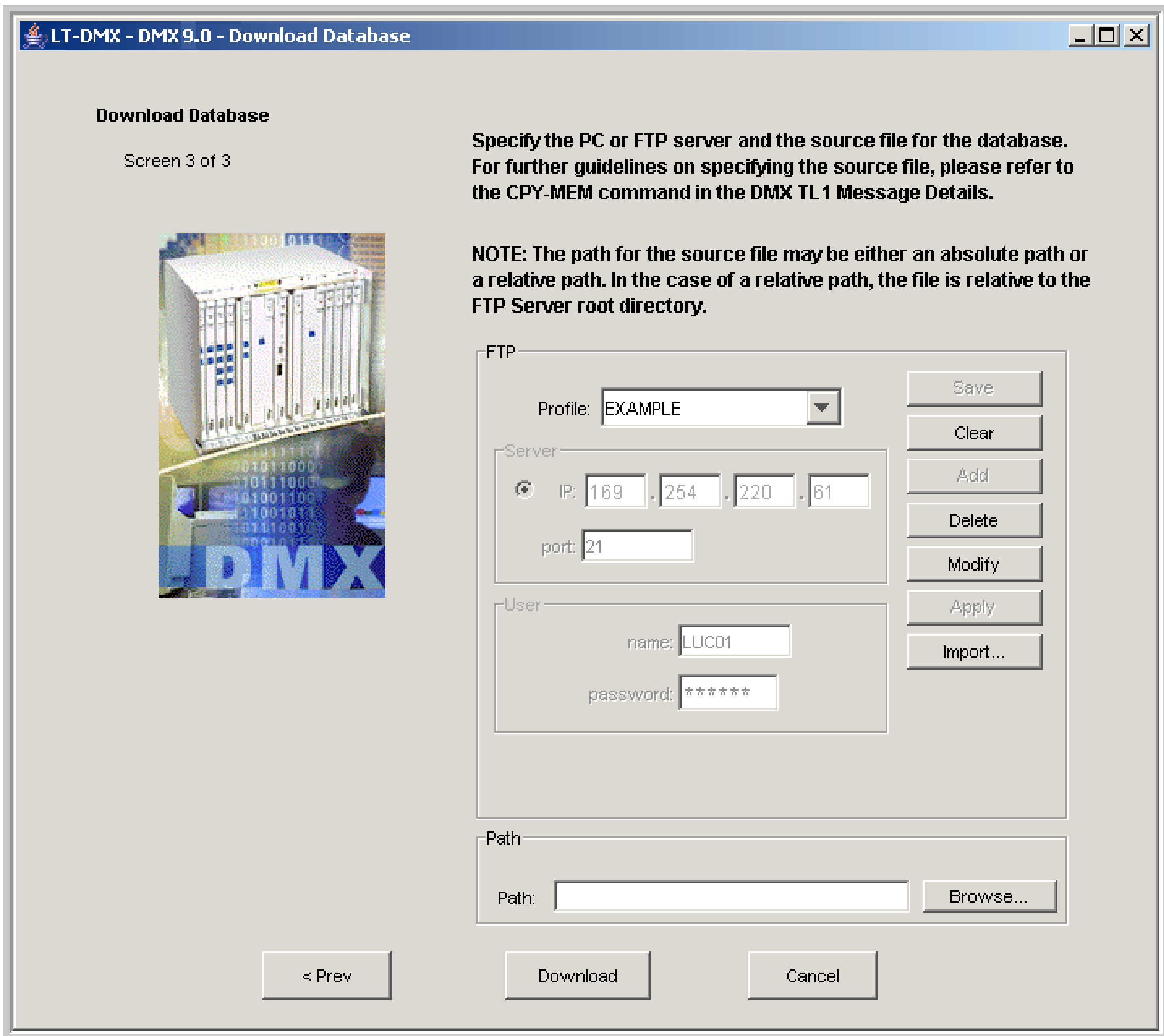


30 **Important!** LAN-1 is the **LAN** port on the faceplate of the LNW2 SYSCTL circuit pack. LAN-2 is the **J16 IAO LAN** port on the rear of the Alcatel-Lucent 1665 DMX shelf.

On Screen 2 of 3 in the Download Database Wizard, the information entered in Step 21 should still be present and valid. If the information is not present, follow the instructions to enable TCP/IP Control on the LAN port to which you are connected. Click **Modify** to enter the IP Address, IP Subnet Mask, and/or IP Default Router Address. If you are connecting directly to the shelf without a router, the IP address of the FTP server must be in the same subnet as the LAN port.

Click **Next**.

Result: Screen 3 of 3 in the Download Database Wizard appears.



31 Select the connection from the **Profile** pull-down menu and proceed to Step 33. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user ID/password may be different.)

32 If you entered connection information in Step 31 and wish to keep the information for future FTP activities:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

Important! Entries to the **Profile** pull-down menu may be changed using the **Modify**, **Apply**, and **Save** buttons or removed using the **Delete** button.

33 On Screen 3 of 3 in the Download Database Wizard in the **Path** panel, enter the location where the database information is stored. Enter the path and filename exactly as it was entered in Step 5. For example: **`\backups\<subdirectory>\<filename>`**.

You may also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and select the required file.

Click **Download**.

Important! The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.

The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is

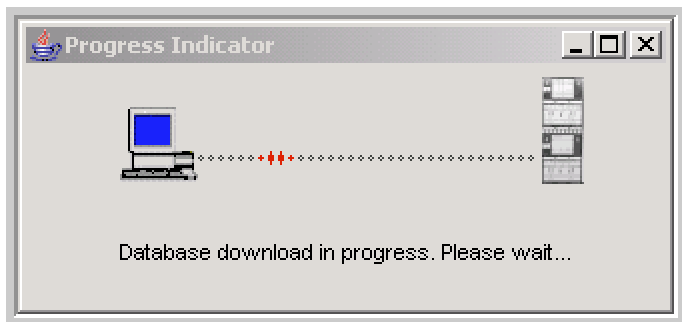
```
C:/Program Files/Alcatel-Lucent/WaveStar CIT/
```

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.

Result: A warning message appears listing the options you provisioned in the previous screens.

34 Verify the information and click **Yes**.

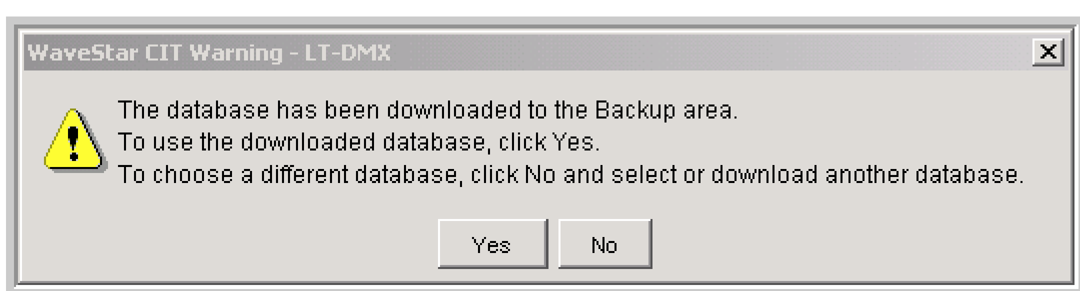
Result: If you choose Yes, the database download progress indicator runs for approximately two minutes.



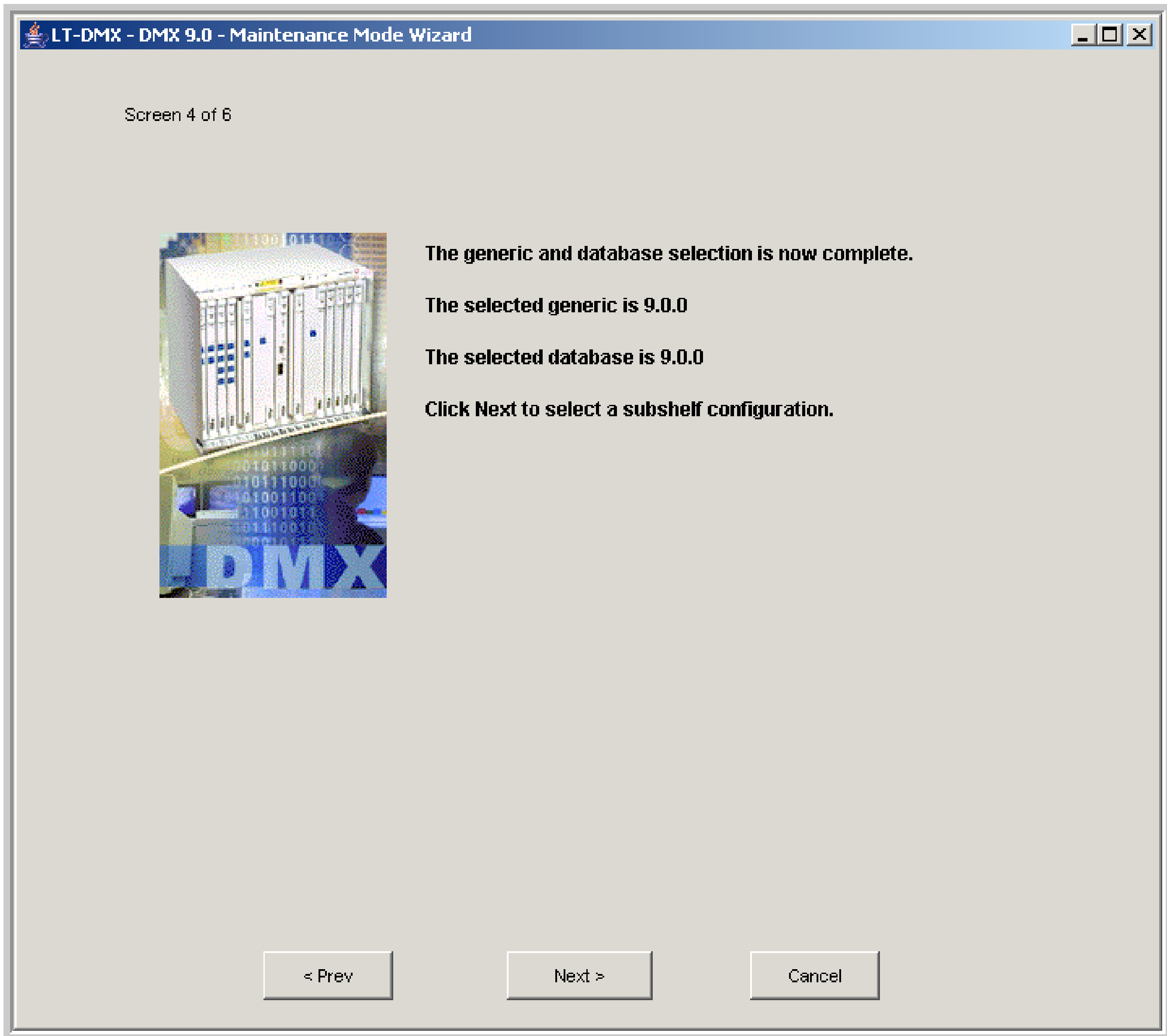
35 Do you wish to observe the FTP download progress?

If...	Then...
Yes	Proceed to Procedure 6-24: "Observe FTP progress" (p. 6-285) and then continue with Step 36.
No	Continue with Step 36.

36 Once the database download is complete, the following confirmation message appears. Click **Yes** to use the database that is now in the Backup area.

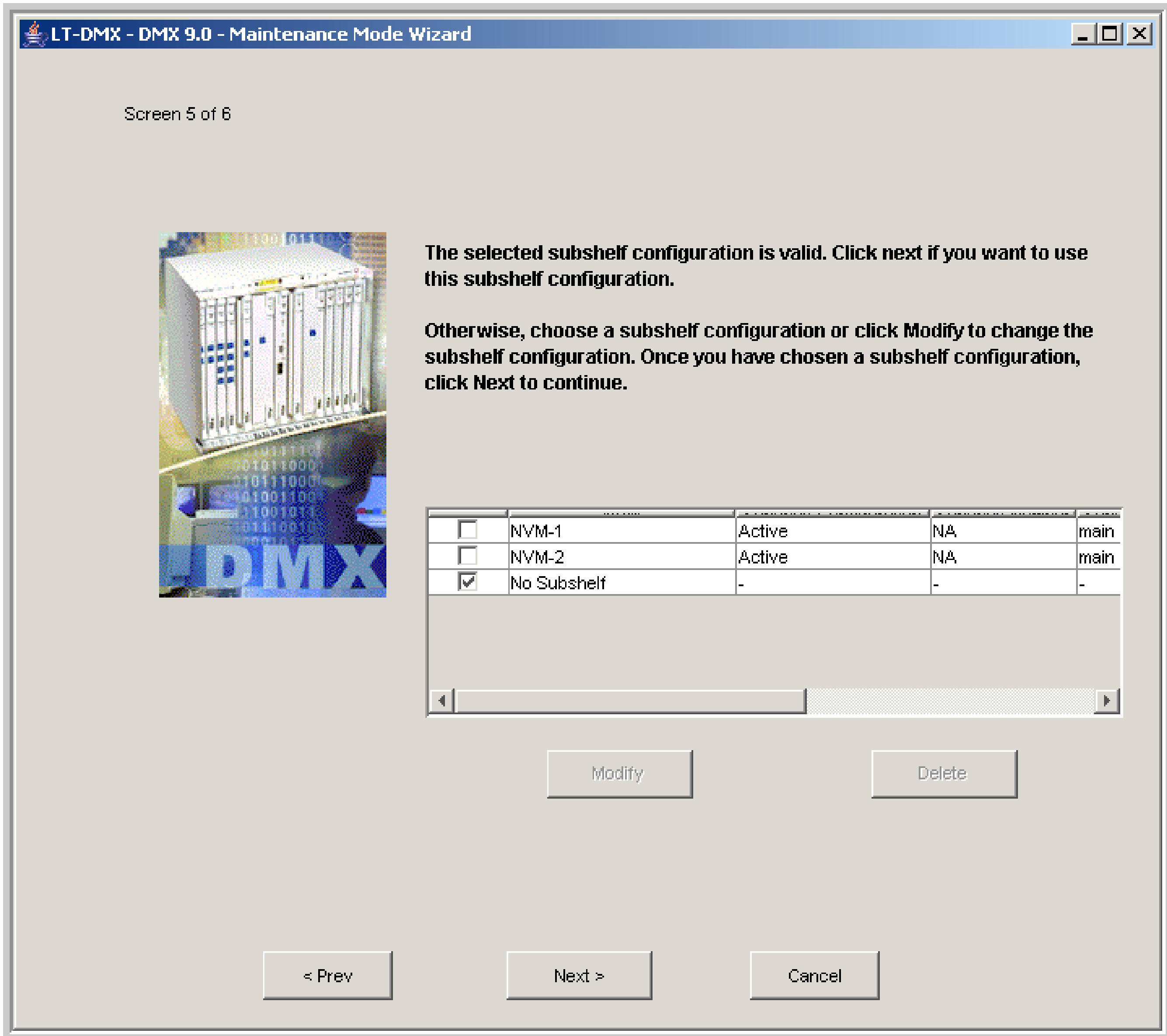


Result: Screen 4 of 6 in the Maintenance Mode Wizard appears. In this screen, 9.1.0 is an example; your selected generic could be different, for example 9.1.1.



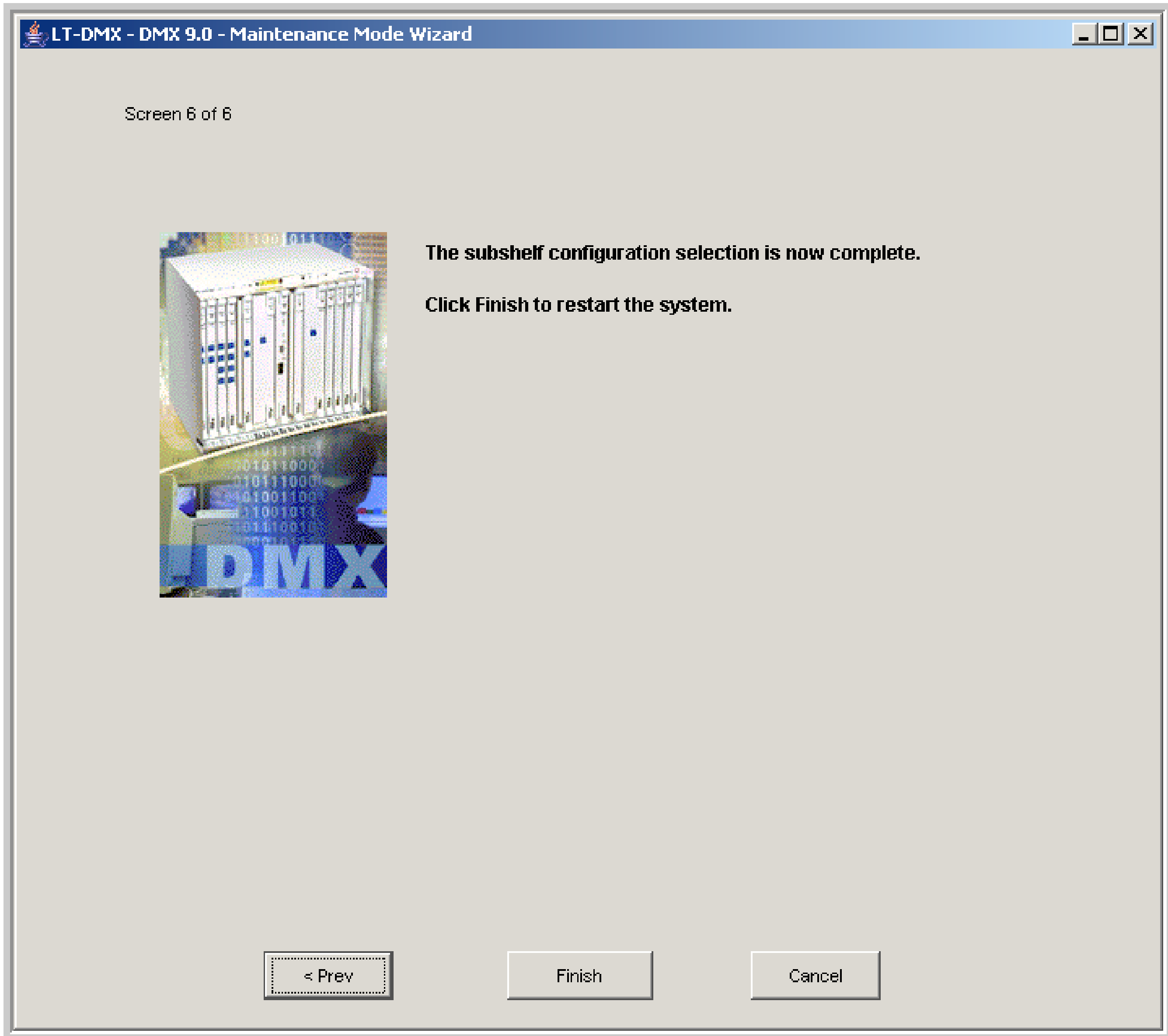
37 On Screen 4 of 6 in the Maintenance Mode Wizard, read the information, verify that you have selected the correct 9.1.x generic and the default database, and click **Next** .

Result: Screen 5 of 6 in the Maintenance Mode Wizard appears.



38 On Screen 5 of 6 in the Maintenance Mode Wizard, select *No Subshelf* or select NVM 1 or 2 if this shelf will be a subshelf and click **Next** .

Result: Screen 6 of 6 in the Maintenance Mode Wizard appears.



39 On Screen 6 of 6 in the Maintenance Mode Wizard, read the information, verify that you have selected the correct generic and database and click **Finish** to restart the system and apply the generic and database.

Result: The Maintenance Mode Wizard closes and your connection to the shelf is terminated.

The LNW2 SYSCTL exhibits the following visible cycles while the generic and database are installed and validated and the SYSCTL reboots:

1. For approximately 20 minutes, the alternating **M** and **P** and **X** (X represents 6, 7, 8, or 9, depending on your Maintenance Mode) and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **Y** (Y represents 0 or 1, depending on your Maintenance Mode) continue to appear in the **IND** display on the SYSCTL.
2. After approximately 12 minutes, all LEDs extinguish and the **IND** display on the SYSCTL is blank for approximately 5 seconds.
3. A flashing **b** appears in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 60 seconds and then **IND** display is blank for approximately 20 seconds.
4. The **ACTIVE** LED lights and remains lighted.
5. A flashing **b** appears again in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 2.5 minutes while the database is being converted and then **IND** display is blank.
6. When nothing appears in the **IND** display and the **ACTIVE** LED is lighted and the other LEDs return to their previous state (pre-backup), the NE software and database installation is complete.

   However, smart circuit packs may be upgrading their firmware. If flashing green **ACTIVE** LEDs are present on a circuit pack, firmware is currently being downloaded to that pack. Wait until all smart circuit packs finish upgrading their firmware before proceeding.

   If an alarm condition existed before the upgrade, the NE rediscovers the alarm condition and activates the appropriate LEDs on the shelf.
7. Continue with Step 40.

40 To verify that the upgrade was successful, depress and hold the **ACO TEST** push-button on the LNW2 SYSCTL for about 4 seconds.

Result: All LEDs on the shelf light. A red, 35-segment (5 x 7) rectangle appears in the **IND** display on the SYSCTL. Since the **IND** display is a 35-segment display, this test indicates all segments are working.

41 Proceed to Procedure 6-10.4: "Verify proper software generic" (p. 6-149).

END OF STEPS

Procedure 6-10.4: Verify proper software generic

Overview

Use this procedure to verify that the proper software generic is active on your SYSCTL and you can log in to the NE.

Required equipment

Refer to "Required equipment" (p. 6-99) in Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99) for a list of equipment required to perform this procedure.

Before you begin

Prior to performing this procedure, complete Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99).

Steps

1 Release the **ACO TEST** push-button on the LNW2 SYSCTL when the red rectangle disappears in the **IND** display.

Result: The current software generic appears in the **IND** display on the LNW2 SYSCTL and the shelf LEDs return to their previous status.

2 From the Network View of the *WaveStar*® CIT session you established in Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99), select the **View:** pull-down menu and select **CIT OSI Neighbors**.

Important! This **View:** is not the menu bar item View → ...; it is located above the NE Name pull-down menu.

3 From the Network View, select **View** → **Refresh OSI View**.

Result: The CIT OSI neighbor(s) are automatically detected.

Your TID will be your original TID, the same TID provisioned on your NE prior to the SYSCTL replacement.

4 In the Network View, right-click the NE icon that was detected, and select **Graphical Using** → **OSI** from the resulting menu.

Result: The *System Type Selection* window appears.

5 In the *System Type Selection* window, select DMX and click **OK**.

Result: The *NE Login Dialog* window appears.

6 In the NE login window, login to the shelf using your original user ID and password; the same user ID and password provisioned prior to the SYSCTL replacement.

Click **OK**.

Result: The title bar of the System View and the legal notice text should both reflect the current NE software generic, for example: 9.1.0.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

7 Is the Generic Software Version correct?

If...	Then...
Yes	STOP! End of Procedure.
No	Contact your next level of support.

END OF STEPS

Procedure 6-11: Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)

Overview

This procedure describes the Alcatel-Lucent recommended method for the cleaning and inspection of optical connectors using specific tools and materials that have been proven to be effective in the assembly and testing of optical transmission equipment.

Required equipment

The following table lists required and recommended equipment for proper cleaning:

Product	Model/ Description	Comcode	ITE #	Installation Order #
Optical Fiber Scope	Noyes OFS 300-200X	408197028	ITE-7129	33712900
2.5mm Universal adapter cap	For use with the Noyes OFS 300-200X	408197044	ITE-7129D1	33712901
1.25mm Universal adapter cap	For use with the Noyes OFS 300-200X	408197069	ITE-7129D2	33712902
Video Fiber Scope*	Noyes VFS-1	408552271	ITE-7187	TBD
CLETOP Cleaning Cassette	Type A Reel	901375154	ITE-7137	33713700
CLETOP Cleaning Cassette Replacement Reel	Type A Reel	901375014	ITE-7137 D1	33713701
Luminex Stick port cleaners	1.25 mm	901375030	ITE-7134	33713400
Luminex Stick port cleaners	2.5 mm	901375022	ITE-7135	33713500
Luminex Cloth	5.5" x 5.5"	408201226	R6033	23603300

* This equipment may not be necessary at all locations. It is to be used when the ports need to be verified for cleanliness. If care is exercised when cleaning fibers, the video scope may not be needed.

Note: The equipment and material listed above has been tested and proven effective when used in conjunction with this procedure. Substitution of equipment or materials is at the discretion of the user and is not recommended.

Related information

A course on connector cleaning and the connector inspection process is now offered through Alcatel-Lucent University, Course Code: LMC214H *Fiber Optic Inspection and Cleaning*. To learn more about this course, consult your local Alcatel-Lucent Account Representative.

The procedure that follows utilizes the *Dry* method for connector cleaning. This method utilizes a dry double clean wipe using the CLETOP cleaning cassette.

This procedure is recommended for connector ferrules 2.5 mm and 1.25 mm in diameter associated with LC connectors. The ferrule of a fiber optic connector consists of a ceramic or stainless steel cylinder with a hole located longitudinally down the center of its axis, allowing enough tolerance for a fiber to pass through.

All optical connectors should be cleaned prior to being connected. Keep the protective ferrule dust cap on the connector until initiating the cleaning process.

> **Important!** It is critical that connector faces are clean and free from particular contamination to assure proper performance and reliability of lightwave systems. With the modern high-speed, high-power, and wider-bandwidth optical transmission systems, clean connectors along the optical path are essential for successful operation.

Before you begin

Prior to performing this procedure:

1. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
2. Obtain the work instructions for this procedure.

Steps

Refer to the following supporting elements to complete this procedure.

1 To clean the optical fibers, refer to Procedure 6-11.1: "Clean optical fibers" (p. 6-153).

2 To clean the fiber adapters and LBOs, refer to Procedure 6-11.2: "Clean fiber adapters and circuit pack connectors" (p. 6-156).

3 To inspect the optics following cleaning, refer to Procedure 6-11.3: "Optical fiber and connector inspection" (p. 6-157).

END OF STEPS

Procedure 6-11.1: Clean optical fibers

Overview

Important! This is *not* a stand-alone procedure. Perform this procedure only as directed by Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151).

Use this procedure to clean optical fibers.

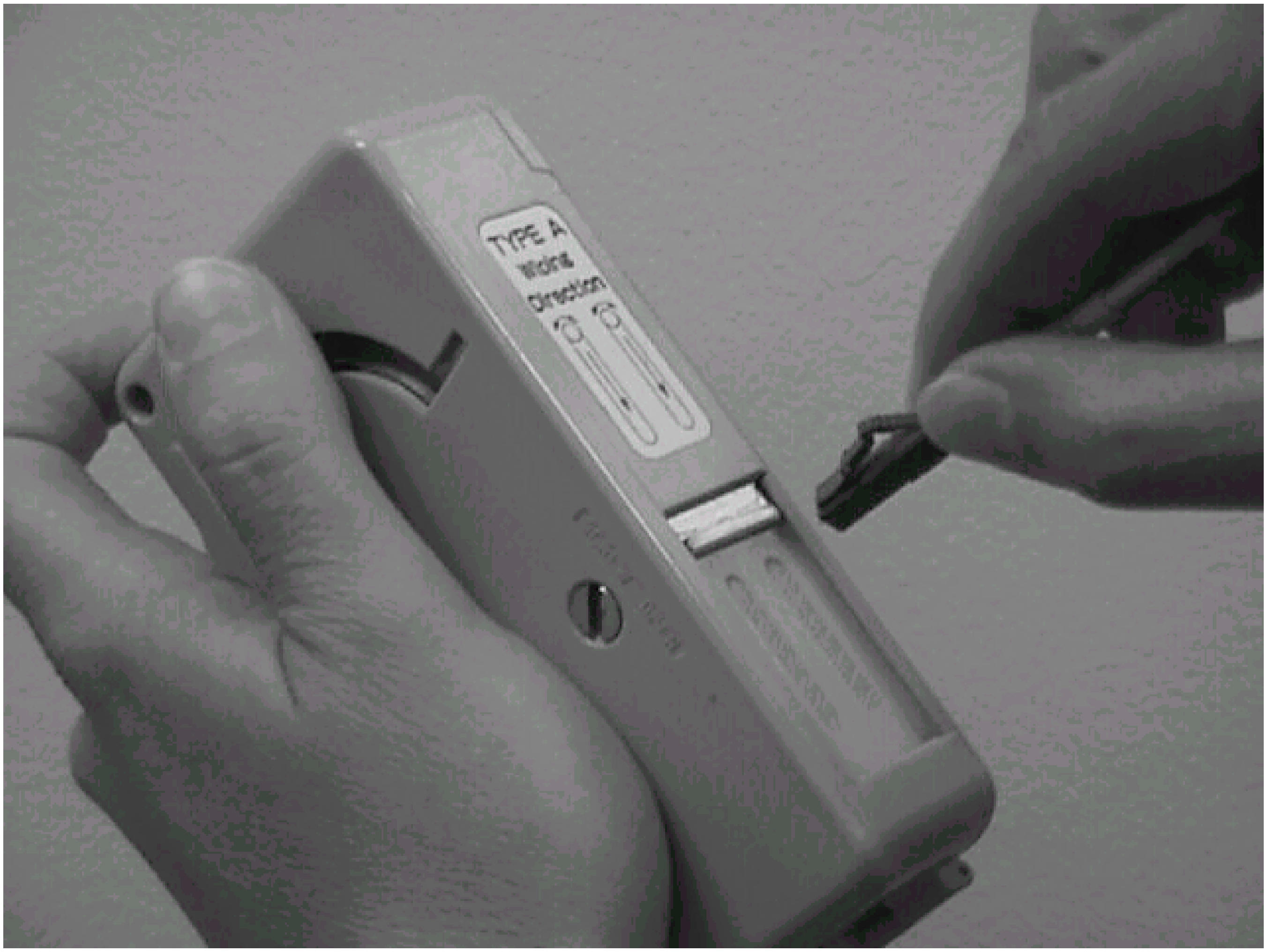
Steps

The following cleaning procedure is acceptable for field service/installation activities.

1 Remove the dust cap from the connector ferrule, thus exposing the connector endface.

2 If a CLETOP cassette cleaner is not available, proceed to Step 6. Otherwise, hold the CLETOP cassette cleaner in the palm of your hand with the cassette shutter door facing up.

Rotate the cassette lever all the way down with your thumb. Do not release the lever. The lever advances the "dry" Luminex cleaning cloth inside the case and simultaneously opens the shutter. The CLETOP cassette shutter door is now open and ready for cleaning the connector.



3 Insert and press the connector ferrule endface perpendicular against the cleaning cloth in the first of two slots of the cleaner.

Drag it down (in the direction indicated by the arrows on the cleaner). Make certain not to release the lever of the cassette.

4 Lift the connector from the first slot and rotate it 90 degrees and repeat the downward motion using the second slot. Be sure the ferrule is pressed snug against the cleaning cloth while dragging the ferrule to assure the proper cleaning action.

5 Release the cassette lever allowing the shutter door to close to its initial position. Proceed to Step 7.

6 Wrap a Luminex cleaning cloth around the ferrule and rotate the connector housing, cleaning the outside periphery of the ferrule.

Follow this by folding an unused portion of the cloth over the end of the ferrule endface and then with light pressure from the thumb, slightly drag the cloth from the center of the ferrule to the edge while rotating the connector 360 degrees. If the Luminex cleaning cloth is not available, a cleanroom optic wipe can be used. The Luminex cleaning cloth is washable and can be used multiple times; optic wipes are single use and disposable.

7 Inspect the connector for cleanliness. If necessary, repeat the cleaning process.

Reference: Procedure 6-11.3: "Optical fiber and connector inspection" (p. 6-157)

END OF STEPS

Procedure 6-11.2: Clean fiber adapters and circuit pack connectors

Overview

Important! This is *not* a stand-alone procedure. Perform this procedure only as directed by Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151).

Use this procedure to clean fiber adapters and circuit pack connectors.

Important! Do not attempt to clean ports equipped with yellow lightguide buildout (LBO) attenuators. Attenuators contain a thin glass lens that is extremely fragile. The LBO will be damaged if cleaned using this method.

Steps

Complete the following steps to clean the optical buildout adapter or the circuit pack connector.

1 Insert the appropriate CLETOP stick cleaner (2.5 mm for SC, ST, and FC connectors, 1.25 mm for LC connectors) into the adapter rotating the stick 360 degrees while inserting. Push/rotate stick until the stick cleaner makes contact with the connector. Apply slight pressure upon contact and rotate stick 360 degrees at least three (3) times.

2 Remove the stick cleaner rotating it upon removal.

3 Using a dry CLETOP stick cleaner of appropriate diameter, repeat the above cleaning procedure. This procedure will clean the side walls of the adapter and the endface of the circuit pack connector.

4 Gently insert the Video Fiber Scope probe into the port until the fiber ferrule comes into view.

Reference: Procedure 6-11.3: "Optical fiber and connector inspection" (p. 6-157)

5 Verify that the fiber ferrule is clean. Repeat Step 1 through Step 3 if the fiber does not meet the requirements specified.

END OF STEPS

Procedure 6-11.3: Optical fiber and connector inspection

Overview

Important! This is *not* a stand-alone procedure. Perform this procedure only as directed by Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151).

Use this procedure to inspect fiber adapters and circuit pack connectors following cleaning.

WARNING

Laser hazard

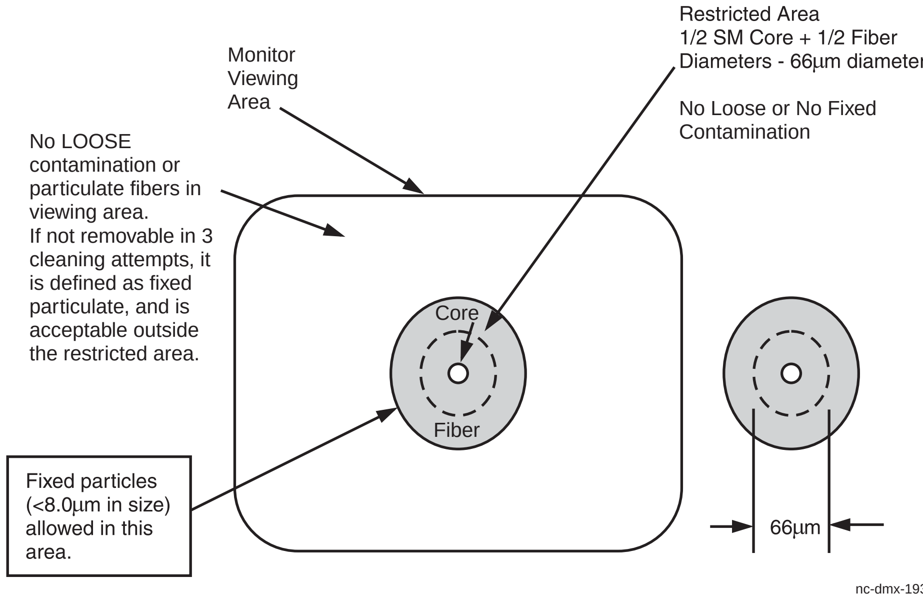
When using an optical power meter to verify the connector and fiber to be clean, take special precaution to make sure that no power is being emitted from the fiber before viewing.

Steps

After cleaning the connector, inspect the ferrule endface to ensure that it is free from any particulate contamination using an optical fiber inspection scope of at least 200X magnification. When using an optical fiber scope (for example, the Noyes OFS 300-200X) exercise extreme caution to assure that the fiber being examined is de-energized.

1 Follow the instructions in the manual provided with the Optical Fiber Scope to view the ferrule endface of the fiber under inspection.

2 The visual area of the ferrule endface (ferrule and fiber) as observed by the inspection system/scope should be free of any contaminates.



Repeat the Cleaning Procedure if the fiber endface does not meet the following requirements:

- No fixed type of contamination (contaminates that remain at the same location after 3 wet-dry cleaning cycles), regardless of size, is allowed in the restricted area of the glass fiber endface.

  Important: The restricted area is defined as ~66 microns (mm) diameter for both singlemode and multimode fibers.
- No chips, cracks or scratches are allowed near the core of the glass fiber endface.
- No large floating (loose) contaminates are allowed on the glass fiber and ceramic ferrule endface.

3 After the connector has been verified to be cleaned, it should be immediately inserted into the adapter buildout of the optical component. This will assure maximum cleanliness and effectiveness of the connector.

4 If the cleaned connector cannot be immediately connected to a corresponding adapter, the connector ferrule must be protected with a connector dust cap. Before placing the cap on the ferrule, make sure the cap is clean. This can be accomplished by inserting a CLETOP stick cleaner (swab) of the same inside diameter as the cap (either 2.5 or 1.25 mm) and rotate the stick 360 degrees three (3) times. Following this procedure, carefully place the cap over the ferrule. When the cleaned connector is ready for assembly, it should be re-inspected for cleanliness prior to connection.

END OF STEPS

Procedure 6-12: Clean optical pluggable transmission module

Overview

This procedure describes the Alcatel-Lucent recommended method for cleaning *uninstalled* optical pluggable transmission modules using specific tools and materials that have been proven to be effective in the assembly and testing of optical transmission equipment.

Important! Pluggable transmission modules are shipped with a dust cover installed into the optical ports to maintain cleanliness during storage and/or transportation. It is recommended that the dust cover be kept in place to maintain cleanliness until the optical fiber is connected. With proper care and handling, cleaning the pluggable transmission modules should not be necessary.

Because a major source of contamination is often a contaminated mating connector, it is extremely important to clean the connector ferrule end surface each time before making connections. To clean the connector ferrule end surface, refer to Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151).

Required equipment

The following equipment is required to perform this procedure.

- CLETOP stick cleaner (1.25 mm for LC connectors)
- Canned dry nitrogen or air (electronics grade)
- Stereo zoom scope with coaxial illumination (200x)

Before you begin

Prior to performing this procedure, refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to clean an optical pluggable transmission module.

1 Remove the protective dust cover from the pluggable transmission module. Keep the dust cover clean until reinstalled later, if required.

2 **NOTICE**

Corrosive-substance hazard

If the canned dry nitrogen or air is held upside down, inert gas may be released onto the connector surface. The inert gas leaves contamination on the connector surface that cannot be removed.

When performing this step hold the canned dry nitrogen or air upright.

While holding the canned dry nitrogen or air, position the tip of the nozzle extension as close as possible, but not close enough to make physical contact, to the sleeve inside the port receptacle and make three consecutive short blows (approximately one second each).

Repeat this step for the other port.

3 Using the stereo zoom scope, visually inspect the pluggable transmission module. If required, repeat Step 2 up to two more times then continue with the next step.

4 **NOTICE**

Equipment damage hazard

Do not perform this step on the receive (RX) port. The receive (RX) port contains a lens for focusing a wide input. The lens is more easily scratched than cleaned.

This step should only be performed on the transmit (TX) port if the air blows did not work.

If required, insert a CLETOP stick into the transmit (TX) port sleeve until vertical force can be applied to the fiber stub end surface. Rotate the CLETOP stick five full rounds.

5 Using the stereo zoom scope, visually inspect the pluggable transmission module. If required, repeat Step 4.

6 **Important!** It is recommended that the dust cover be installed into the optical ports on the pluggable transmission module to maintain cleanliness until the optical fiber is connected.

If required, reinstall the dust cover into the optical ports to maintain cleanliness.

END OF STEPS

Procedure 6-13: Install/remove LC lightguide buildouts (LBOs)

Overview

Use this procedure to install or remove an LC lightguide buildout (LBO).

Before you begin

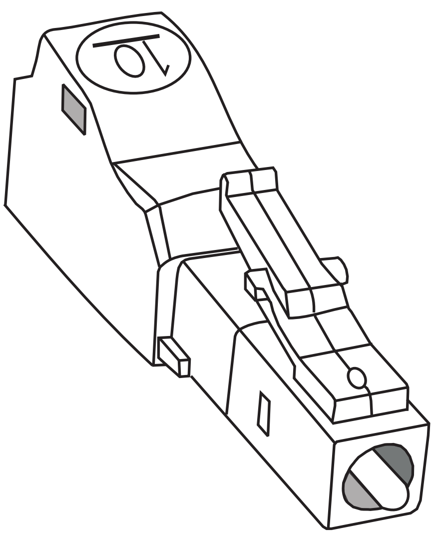
Prior to performing this procedure:

1. Refer to "Before you begin" (p. 6-3) and "Required equipment" (p. 6-3) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
3. Obtain the work instructions for this procedure.

Steps

Complete the following steps to install or remove an LC lightguide buildout (LBO).

1 Remove the protector caps and plugs (if equipped) from the LC LBO and the dual adapter on the circuit pack, and store them in a clean container.



MA-DMX-403

2 Is LC LBO being installed or removed?

IF the LC LBO is being...	Then...
Installed,	Continue with Step 3.
Removed,	Proceed to Step 6.

3 **Important!** All LC LBOs should be cleaned before making initial connections or reconnections. Only the components being assembled at this time should be cleaned.

Clean the LC LBO.

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

4 Align the LBO with the slot in the adapter, depress locking tab, and push the LBO into the dual adapter until a click is heard. The LBO is now locked into position.

5 STOP! End of Procedure.

6 **Important!** The locking tab must only be pushed along a line perpendicular to the LBO body in the direction towards the LBO in order to avoid damage to the locking tab.

Depress the locking tab on the LBO and pull the LBO out of the dual adapter.

END OF STEPS

Procedure 6-14: Connect OLIU optical loopbacks

Overview

Use this procedure to loop back an *out-of-service* optical line at the OLIU faceplate connectors. Optical lines can also be looped back at the LGX equipment to verify correct fiber installation and labeling.

Important! LBOs are installed on the OLIU faceplate **IN** connector only.

Required equipment

In addition to the equipment listed in "Required equipment" (p. 6-3), one lightguide jumper (MS1A40LC-A40LC-2, Comcode 108918269) for each optical line to be looped back (LC-type connections) is also required.

The following lightguide buildouts (LBOs) are required.

- 5-dB loss LBO (code ABLCS-05.0: comcode 108279381) or
- 10-dB loss LBO (code ABLCS-10.0: comcode 108279431) or
- 15-dB loss LBO (code ABLCS-15.0: comcode 108279480) or
- 20-dB loss LBO (code ABLCS-20.0: comcode 108279530)

Before you begin

Prior to performing this procedure:

1. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
2. Obtain the work instructions for this procedure.

Steps

Complete the following steps to loop back an *out-of-service* optical line at the OLIU faceplate connectors.

1 Obtain the correct LBO and lightguide jumper:

If the OLIU is...		**Then obtain a...**
Long Reach (LR) Optics	LNW36 OC-3	lightguide jumper (MS1A40LC-A40LC-2, Comcode 108918269) and a **10-dB** LBO (code ABLCS-10.0, comcode 108279431 for LC connectors)
	LNW26B OC-48 LNW27 OC-48 LNW28 OC-48 LNW29 OC-48 LNW32 OC-48 LNW121B–159B OC-48 LNW221–259 OC-48 LNW421–459 OC-48	lightguide jumper (MS1A40LC-A40LC-2, Comcode 108918269) and a **15-dB** LBO (code ABLCS-15.0, comcode 108279480 for LC connectors)
	LNW46 OC-12 LNW50 OC-12	
	LNW54 OC-12 LNW555 OC-192 LNW57 OC-192 LNW60 OC-192 OM155 1.3LR1 OM622 1.3LR1 OM622 1.5LR2 OM2.5G 1.3LR1 OM2.5G 1.5LR2 OM10G 1.5LR2	lightguide jumper (MS1A40LC-A40LC-2, Comcode 108918269) and a **20-dB** LBO (code ABLCS-20.0, comcode 108279530 for LC connectors)

If the OLIU is...		**Then obtain a...**
Intermediate Reach (IR) Optics	LNW31 OC-48 LNW48 OC-12 LNW56 OC-192 LNW77 OC-48 LNW523 OC-192 LNW527 OC-192 LNW554 OC-192 OM155 1.3IR1 OM622 1.3IR1 OM10G 1.5IR2	lightguide jumper (MS1A40LC-A40LC-2, Comcode 108918269) and a **5-dB** LBO (code ABLCS-05.0, comcode 108279381 for LC connectors)
Short Reach (SR) Optics	LNW76 OC-48 LNW58 OC-192 OM155 1.3SR1 OM2.5G 1.3SR1 OM10G 1.3SR1	No LBO required (attenuation not needed)

2 If required, remove the optical line connections from the OLIU faceplate. Make a record of these disconnections so they can be replaced.

3 Remove the LBO (if equipped) from the **IN** connector of the OLIU faceplate. Make a note of the value.

Reference: Procedure 6-13: “Install/remove LC lightguide buildouts (LBOs)” (p. 6-162)

4 Remove the protector caps from the ends of the lightguide jumper (loopback cable).

5

NOTICE

Service-disruption hazard

Signal performance may be degraded if the connectors/adapters and fiber are not cleaned.

Ensure all optical fiber connectors/adapters and fiber are properly cleaned.

Clean the fiber connectors/adapters and fiber.

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

6 **Important!** Pluggable transmission modules are shipped with a dust cover installed into the optical ports to maintain cleanliness during storage and/or transportation. It is recommended that the dust cover be kept in place to maintain cleanliness until the optical fiber is connected. With proper care and handling, cleaning the pluggable transmission modules should not be necessary.

If required, clean the pluggable transmission module(s).

Reference: Procedure 6-12: "Clean optical pluggable transmission module" (p. 6-160)

7 If required, remove the protective dust cover from the pluggable transmission module. Keep the dust cover clean until reinstalled later, if required.

8 Install the appropriate LBO on the **IN** connector, if required. The list of circuit packs and their corresponding LBOs may be found in Step 1.

Reference: Procedure 6-13: "Install/remove LC lightguide buildouts (LBOs)" (p. 6-162)

9 **Important!** The LBOs and lightguide jumpers connect to the LC-shielded, angled adapter on the OLIU faceplate.

Using the lightguide angled boot jumper (MS1A40LC-A40LC-2, Comcode 108918269), connect the **IN** connector and the corresponding **OUT** connector on the same OLIU.

Result: After a short time, the OLIU **FAULT** LED or port LED associated with the pluggable transmission module stops flashing. (It may take from 15 seconds to 3.5 minutes for the LED to stop flashing after the cables are connected, depending on the setting of the OC-n signal degrade threshold.) The **ACTIVE** LED remains on.

If OSI over DCC is enabled for the port, the **MJ** and **NE** LEDs on the SYSCTL circuit pack do *not* extinguish and the following alarms are reported.

- inconsistent DCC values
- section DCC channel failed

10 If responses are not as indicated, check connections and the lightguide jumper. Clean connections and repeat Step 9.

If responses are still not correct, click the **Alarm List** button to obtain the *NE Alarm List*. Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Alarm Messages and Trouble Clearing Guide, 365-372-302* to clear/isolate the trouble.

Reference:

- Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)
- Procedure 6-12: "Clean optical pluggable transmission module" (p. 6-160)

11 If required, repeat Step 1 through Step 10 to loop back additional optical lines.

END OF STEPS

Procedure 6-15: Replace fan filter

Overview

Use this procedure to replace a fan filter.

Important! In central office applications, the fan shelf must equipped with a fan filter. To keep the fan shelf operating properly, it is recommended that users routinely change the fan filter every 6 to 9 months.

In outside plant (OSP) applications, remove the fan filter. Operating Alcatel-Lucent 1665 DMX in an OSP without the fan filter improves air flow and therefore enhances cooling performance and extends the life of the equipment.

Required equipment

The following equipment is required:

- Wrist Strap
- A replacement filter
  - For Alcatel-Lucent 1665 DMX Comcode: 408 456 770
  - For Alcatel-Lucent 1665 DMX High Capacity shelf Comcode: 408 682 615

Before you begin

Prior to performing this procedure:

1. Refer to “Before you begin” (p. 6-3) in this chapter
2. Refer to “Electrostatic discharge” (p. 1-26) in Chapter 1, “Safety”
3. Ensure that the replacement fan filter is the same type as the original fan filter.
4. Note that the Standard Shelf is Discontinued Availability effective 6/30/04.

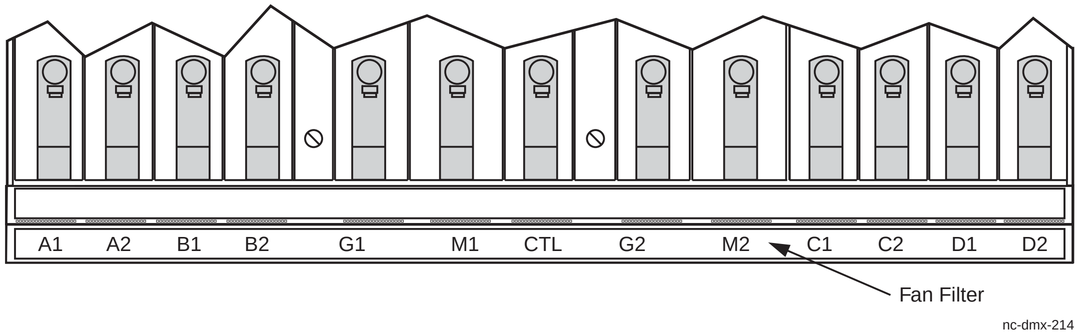
Steps

Complete the following steps to replace the fan filter.

1 Remove the fan filter by pulling it towards you.

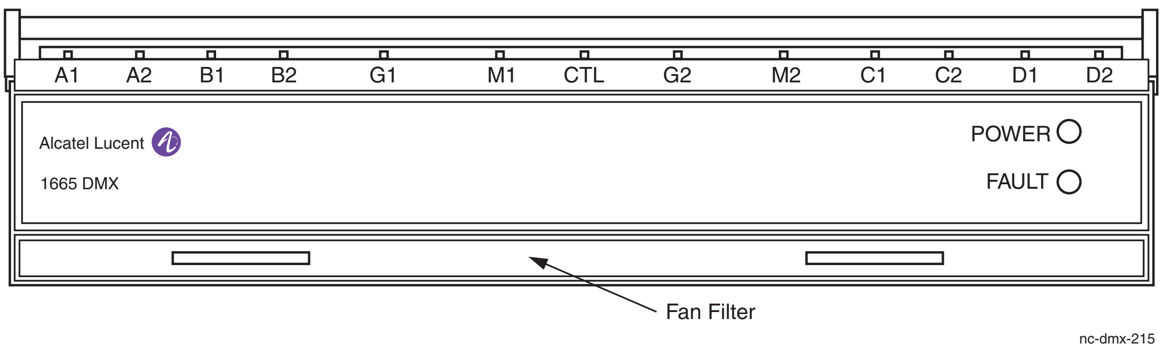
In the Alcatel-Lucent 1665 DMXstandard shelf, the fan shelf is installed above the shelf. However, fan filter is located below the shelf, under the Alcatel-Lucent 1665 DMX fiber tray (see Figure 6-22, “Alcatel-Lucent 1665 DMX Standard Shelf fan filter” (p. 6-170)).

Figure 6-22 Alcatel-Lucent 1665 DMX Standard Shelf fan filter



In the Alcatel-Lucent 1665 DMX High Capacity shelf, the fan shelf is installed below shelf. The fan filter is located directly below the fan shelf (see Figure 6-23, "Alcatel-Lucent 1665 DMX High Capacity shelf fan filter" (p. 6-170)).

Figure 6-23 Alcatel-Lucent 1665 DMX High Capacity shelf fan filter



2 Install new filter into the fan filter slot.

E N D O F S T E P S

Procedure 6-16: Ugrade software generic via SFTP

Overview

Use this procedure to upgrade the software generic from Release 9.0.1 to 9.1.x via SSH FTP (SFTP). Replace 9.1.x with your current release, for example 9.1.1.

Important! Your NE must be running Release 9.0.x or later to use this procedure.

Important! When performing this software upgrade, you may experience transmission hits within typical protection switch times (up to 60 ms).

To download the software generic to a remote shelf using SFTP, refer to Procedure 6-16: "Ugrade software generic via SFTP" (p. 6-171).

To download the software generic to a remote shelf using FTP, refer to Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175).

To download the software generic to a remote shelf using FTTD, refer to Procedure 6-18: "Upgrade software generic via FTTD" (p. 6-212).

To download the software generic to a local or remote shelf using FTAM, refer to Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218).

Note: You must have direct TCP/IP connectivity to your NE and the NE must have a defined IP address.

Privilege level

You must log in as a Privileged user to complete this procedure.

Required equipment

In addition to "Description" (p. 3-14) listed in this chapter, the following equipment is also required:

- CAT5 Ethernet cable with either a 10/100 hub or a cross-over cable for the **LAN** port.
- Copy of the new system generic software program on your SFTP server.
- Current Alcatel-Lucent 1665 Data Multiplexer (DMX) Software Release Description for the software generic being installed.

Before you begin

Prior to performing this procedure:

1. Refer to "Description" (p. 3-13) in this chapter and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
2. Verify that the new software generic program is available.
3. Refer to the Alcatel-Lucent 1665 Data Multiplexer (DMX) Software Release Description for the software being downloaded for a description of any special considerations involving this version of software.

If you log in using TCP/IP, your PC must be part of the GNE's TCP/IP Gateway Host List. Refer to Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301.

Steps

Complete the following steps to download system software using SFTP.

1 Establish a *WaveStar*® CIT session (depending on the physical connection used) and log in to the destination shelf (the shelf to which you want to download the software) in your network.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

2 From the System View menu, select **View** → **Software Generic**.

3 Is the Active Software Version 9.0.1 or later?

If...	Then...
Yes	Continue with Step 4.
No,	You must upgrade your software to Release 9.0.1 and then repeat this procedure from Step 1.

4 From the System View menu, select **Configuration** → **Software** → **Download Software**.

Result: The *Download Software* window opens.

5 In the pull-down **Download From/Via:** menu, select **SFTP**. Select a connection profile from the **Profile** pull-down menu and proceed to Step 7. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the SFTP server.
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 22 is valid if entered.
3. In the **User** panel, enter the user name and password for the SFTP server.

6 If you entered connection information in Step 5 and wish to keep the information for future backups:

1. Enter a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

Important! Entries to the **Profile** pull-down menu may be changed using the **Modify**, **Apply,** and **Save** buttons or removed using the **Delete** button.

7 In the **Source/Destination Directory Path** panel, enter the path starting at the SFTP home directory on the server.

8 Click **OK**.

Result: A warning message appears indicating the transfer you are about to execute. *Do you wish to continue?* Verify the information and click **Yes**. While the download is in progress, a *Progress Indicator* window is present.

The download takes approximately 5 minutes.

The download may be cancelled any time by clicking **Cancel** on the *Progress Indicator* window.

When the transfer is complete, the *Progress Indicator* window closes and the download software successful screen appears. Click **OK**.

9 **Important!** Do NOT insert a new circuit pack in the shelf until after you apply the new software generic and clear the `dormant/exec version mismatch` condition.

Do you wish to apply (activate) the software generic that you recently downloaded to the dormant area of the Alcatel-Lucent 1665 DMX shelf?

If...	Then...
Yes	Proceed to Procedure 6-20: "Apply software generic" (p. 6-249) and then continue with Step 10.
No	Continue with Step 10.

10 Do you wish to upgrade additional shelves using SFTP?

If...	Then...
Yes	Repeat this procedure from Step 1 for each shelf that you wish to upgrade using SFTP.
No	STOP! End of Procedure.

END OF STEPS

Procedure 6-17: Upgrade software generic via FTP

Overview

Use this procedure to upgrade the software generic to Release 9.1.x via File Transfer Protocol (FTP).

Note: You can upgrade directly to 9.1.x from the following releases:

- R5.1.3/5.1.7
- R7.1.2
- R8.0.2/R8.0.3/8.0.4/8.0.5/8.0.6
- R9.0.1

You must complete a two-step upgrade to 9.1.x from the following releases:

- R6.0.1/6.0.2/6.0.4 through R8.0.5
- R7.0.2 through R8.0.5
- R7.1.1/7.1.4 through R8.0.6

You must complete a three-step upgrade to 9.1.x from R5.1.4/5.1.5 through R7.0.2, and then through R8.0.5.

To download the software generic to a local shelf via FTAM, refer to Procedure 6-19: “Upgrade software generic via FTAM” (p. 6-218).

Important! You must have direct TCP/IP connectivity to your NE and the NE must have a defined IP address.

Privilege level

You must log in as a Privileged user to complete this procedure.

Required equipment

In addition to “Required equipment” (p. 6-3) listed in this chapter, the following equipment is also required:

- CAT5 Ethernet cable with either a 10/100 hub or a cross-over cable for the **LAN** or **IAO LAN** port
- Copy of the new system generic software program on your PC or FTP server
- Current *Alcatel-Lucent 1665 Data Multiplexer (DMX) Software Release Description* for the software generic being installed

  Important! If the FTP server fails to start, it could mean that another program using an FTP server is already running. Depending on what operating system you are using, you must go to the device file and disable the FTP server. Refer to Procedure 6-25: “Disable an FTP server on your PC” (p. 6-287) for instructions for each allowed operating system.

Before you begin

Before performing this procedure:

1. Refer to "Before you begin" (p. 6-3) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
2. Verify that new software generic program is available.
3. Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Software Release Description* for a description of any special considerations required when installing this version of software.

Steps

Complete the following steps to upgrade the software generic via FTP.

1 Connect the cross-over LAN cable from the Network Interface Card (NIC) on the PC to the rear **J16 IAO LAN** port on the Alcatel-Lucent 1665 DMX shelf backplane or the front **LAN** port on the SYSCTL circuit pack faceplate and establish a *WaveStar*® CIT session. (When TCP/IP is enabled on the rear LAN port, OSI is disabled.)

Double-click the *WaveStar*® CIT icon on your desktop and login (if necessary), to start the *WaveStar*® CIT software on the PC. Refer to Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27).

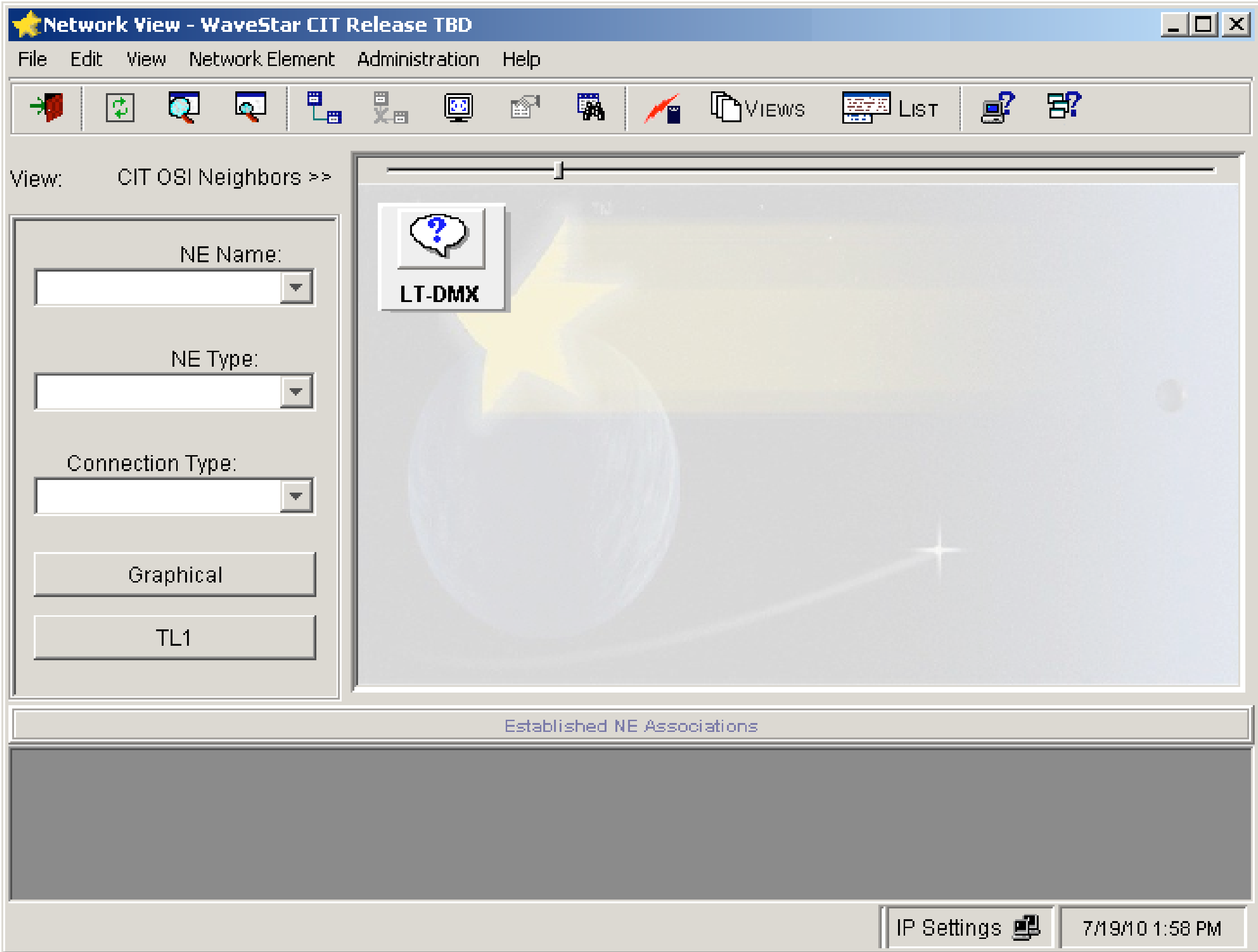
Result: The *Network View* appears.

2 From the **View:** pull-down menu, select **CIT OSI Neighbors**.

Important! This **View:** is not the menu bar item View → ...; it is located above the NE Name pull-down menu.

Result: The CIT OSI neighbor(s) are automatically detected.

If you were previously logged in to the NE and/or you do not see your NE, from the Network View, select **View** → **Refresh OSI View**.



3 In the Network View, right-click the NE icon that was detected (default TID is LT-DMX, your TID can be different), and select **Graphical Using** → **OSI** from the resulting menu.

Result: The *System Type Selection* window appears.

4 In the *System Type Selection* window, select DMX and click **OK**.

Result: The *NE Login Dialog* window appears.

5 In the NE login window, login to the shelf using your user ID and password. Click **OK**.

6 From the System View menu, select **View** → **Equipment**, highlight the SYSCTL, and click **Select**.

Result: The *View Equipment* window appears. Record the Apparatus Code and the Program Version.

7 What is the apparatus code of your SYSCTL and what program version (software generic Release x.x.x) is it currently running?

If...	Then...
Apparatus Code = LNW1 Program Version = 3.1, 4.0, 5.0	You must upgrade your software to Release 5.1.3 and then repeat this procedure from Step 1.
Apparatus Code = LNW1 Program Version = 5.1.3/5.1.7	Proceed to Procedure 6-17.1: "Verify proper equipage in Main slots" (p. 6-179).
Apparatus Code = LNW1 Program Version = 5.1.4/5.1.5	You must upgrade your software to Release 7.0.2 and then repeat this procedure from Step 1.
Apparatus Code = LNW2 Program Version = 6.0.x (x=1, 2, 4) or 7.0.2	You must upgrade your software to Release 8.0.6 and then repeat this procedure from Step 1.
Apparatus Code = LNW2 Program Version = 7.1.x (x=1, 2, 4)	You must upgrade your software to Release 7.1.2 and then repeat this procedure from Step 1.
Apparatus Code = LNW2 Program Version • 7.1.x (x=1, 2, 4) • 8.0.x (x=2, 4, 5, 6) • 9.0.1	Proceed to Procedure 6-17.3: "Upgrade software generic via FTP (7.1.x, 8.0.x, 9.0.1 or later to 9.1.x)" (p. 6-207).

END OF STEPS

Procedure 6-17.1: Verify proper equipage in Main slots

Overview

Use this procedure to verify that the Main slots are equipped with circuit packs that are supported in 9.1.x.

LNW26 circuit packs are not supported in 9.1.x.

Since LNW26B-type circuit packs with the jumper set to *NORMAL* are identical to LNW26 circuit packs, LNW26B-type circuit packs (LNW26B, LNW28, LNW77, LNW121B-151B) with the circuit pack mode jumper set to *NORMAL* (six STS-1 switch fabric) are not supported in 9.1.x. The jumper on LNW26B-type circuit packs must be set to *ENHANCED* (12 STS-1 switch fabric) to use these circuit packs in 9.1.x.

> **Important!** If you determine that the Main slots in your NE are equipped with unsupported circuit packs, you must upgrade those circuit packs before upgrading to 9.1.x.

Required equipment

Refer to "Required equipment" (p. 6-175) in Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure:

1. Complete Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175).
2. If your Main slots contain unsupported circuit packs, you must have access to supported circuit packs.

Steps

Complete the following steps to verify that supported equipment is installed in your shelf.

1 From the System View menu, select **Reports** → **Equipment Lists** → **Pack**, highlight **Shelf**, and click **Select**.

Result: The *Circuit Pack List* screen appears.

2 In the *Circuit Pack List* screen, locate the *main-1-cp* and *main-2-cp* AIDs in the Circuit Pack AID column. Are the Apparatus Codes for those AIDs either LNW26 or LNW26B-type (LNW26B, LNW28, LNW77, LNW121B-151B)?

If...	Then...
Yes (LNW26)	You must upgrade the LNW26 circuit packs in the Main slots to supported circuit packs. Refer to *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* for detailed instructions about upgrading circuit packs and then repeat this procedure.
Yes (LNW26B, LNW28, LNW77, LNW121B-151B)	Continue with Step 3 to determine the circuit pack mode of the packs.
No	The Main slots are equipped with circuit packs that are compatible with 9.1.x. Proceed to Procedure 6-17.2: "Upgrade software generic via FTP (5.1.3/5.1.7 to 9.1.x)" (p. 6-182).

3 From the System View menu, select **View** → **Equipment** → **Circuit Pack**, highlight CP main-1, and click **Select**.

Result: The *View Equipment* screen appears.

4 In the *View Equipment* screen, locate the Circuit Pack Mode parameter in the Equipment Details panel. Note the value of the Circuit Pack Mode for CP Main-1, either *NORMAL, or ENHANCED*.

Do NOT click **Close** on the *View Equipment* screen.

5 Highlight CP main-2 and click **Select**.

6 In the *View Equipment* screen, locate the Circuit Pack Mode parameter in the Equipment Details panel. Note the value of the Circuit Pack Mode for CP Main-2, either *NORMAL, or ENHANCED*.

7 Refer to Step 4 and Step 6. Is the Circuit Pack Mode for CP main-1 and/or CP main-2 *NORMAL* (six STS-1 switch fabric)?

If...	Then...
Yes	The LNW26B-type circuit packs with the Circuit Pack Mode jumper set as *NORMAL* are NOT supported in 9.1.x. Choose one of the following two options: 1. Change Circuit Pack Mode to *ENHANCED* by physically changing the jumper setting on the circuit packs. Proceed to Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48) for detailed instructions on changing jumper settings and then repeat this procedure. 2. Upgrade the LNW26B-type circuit packs to LNW27, LNW29, LNW32, LNW76, LNW202, or LNW221–259 OC-48 OLIU circuit packs. These circuit packs can cross-connect VT1.5 signals in up to 48 STS-1 signals. Refer to *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* for detailed instructions about upgrading circuit packs and then repeat this procedure.
No	The LNW26B-type circuit packs with the Circuit Pack Mode jumper set as *ENHANCED* are supported in 9.1.x. Proceed to Procedure 6-17.2: "Upgrade software generic via FTP (5.1.3/5.1.7 to 9.1.x)" (p. 6-182) to upgrade the 5.1.x shelf to 9.1.x.

END OF STEPS

Procedure 6-17.2: Upgrade software generic via FTP (5.1.3/5.1.7 to 9.1.x)

Overview

Use this procedure to upgrade a software generic from Release 5.1.3/5.1.7 to Release 9.1.x via FTP.

Required equipment

Refer to "Required equipment" (p. 6-175) in Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure:

1. Complete Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175).
2. You must be able to perform a backup of the LNW1 database.

Steps

Complete the following steps to upgrade a software generic from Release 5.1.3/5.1.7 or later to Release 9.1.x via FTP.

1 From the System View menu, select **Configuration** → **Software** → **Remote Backup**.

2 In the pull-down **Backup To/Via:** menu, select **FTP**.

3 Select the connection from the **Profile** pull-down menu and proceed to Step 5. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user ID/password can be different.)

4 If you entered connection information in Step 3 and wish to keep the information for future backups:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

   Entries to the **Profile** pull-down menu can be changed using the **Modify**, **Apply**, and **Save** buttons or removed using the **Delete** button.

5 In the **Source/Destination Directory Path** field, enter **`\backups\<filename>`** if you wish to save the backup file to the default location. (If the *WaveStar*® CIT is the FTP server, a maximum of 80 characters is suggested for this field.)

You can also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and over-write the default entry. The **Browse** button is not available (greyed out) if the FTP server is not the local *WaveStar*® CIT or the IP address of the FTP server is not in the same subnet as the IP address of the shelf.

> **Important!** The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.
>
> The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is
>
> `C:\Program Files\Alcatel-Lucent\WaveStar CIT\`
>
> If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.
>
> If you wish to store your data in a subdirectory, enter **`\backups\<subdirectory>\<filename>`** if the subdirectory exists before the command is sent. If any directory in the path does not exist, the command is denied because this command does not create directories.

6 Click **OK**.

You are asked to verify that you wish to backup to the directory that you entered. Click **Yes** if you typed the path correctly.

Result: The *Progress Indicator* screen appears, indicating that the backup is in progress. When the backup completes, a `Remote Backup successful` screen appears. Click **OK**. The backup file is now stored. If the default path and a subdirectory were used, the file can be found at:

```
C:/Program Files/Alcatel-Lucent/WaveStar CIT/backups/
<subdirectory>/<filename>
```

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.

7 Close your *WaveStar*® CIT session with the 5.1.x NE. From the System View, select **File** → **NE Disconnect** and click **Yes** in the confirmation window.

Result: The *System View* closes.

8 Disconnect the LAN and/or serial cables from the **LAN** and/or **RS232** port(s) on the front of the LNW1 SYSCTL.

9 Initiate a ten-second countdown (9, 8, 7, 6, 5, 4, 3, 2, 1, 0) in the **IND** display on the LNW1 SYSCTL by simultaneously depressing the **ACO TEST** and **SEL** buttons on the front of the LNW1 SYSCTL.

Important! Removing the LNW1 without initiating the ten-second countdown can result in unexpected and undesirable protection switches, incorrect circuit fault indications, or incoming signal failure alarms. All SYSCTL functions are suspended during the countdown.

10 Remove the LNW1 SYSCTL circuit pack during the 10-second countdown.

Important! While the SYSCTL circuit pack is removed, do *NOT* remove or replace any transmission circuit packs.

11 **Important!** For software installation, ensure that two NVMs are present in the LNW2 SYSCTL. After the LNW2 is installed, if one or two NVMs are missing, `NVM removed` alarm(s) are issued. If both NVM sockets are empty, the **IND** displays an alternating **E** and **0** and **1**.

Refer to Step 12 for the complete listing of codes and required actions.

Seat the new LNW2 SYSCTL circuit pack and allow a few minutes for the pack to complete initialization.

Result: The LNW2 SYSCTL exhibits the following visible cycles during initialization:

1. The **FAULT** LED lights and remains lighted for approximately 90 seconds. After approximately 10 seconds, a flashing **b** appears in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 75 seconds and the **IND** display is blank.
2. The **FAULT** LED remains lighted for approximately another 20 seconds and then extinguishes.
3. The **ACTIVE** LED lights and remains lighted and the **CR** LED flashes 10 times. While the **CR** LED is flashing, the **MJ**, **ABN**, and **NE** LEDs light and remain lighted.
4. Continue with Step 12.

12 Observe the **IND** display on the LNW2 SYSCTL; the display indicates the state of the SYSCTL.

If...	Then...
alternating **M** and **P** and **6** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	6.0 Maintenance Mode. Continue with Step 13.
alternating **M** and **P** and **7** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	7.0 Maintenance Mode. Continue with Step 13.
alternating **M** and **P** and **7** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **1**	7.1 Maintenance Mode. Continue with Step 13.
alternating **M** and **P** and **8** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	8.0 Maintenance Mode. Continue with Step 13.
alternating **M** and **P** and **9** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	9.0 Maintenance Mode. Continue with Step 13.
alternating **M** and **P** and **9** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **1**	9.1 Maintenance Mode. Continue with Step 13.
alternating **E** and **0** and **0**	LNW2 SYSCTL must be replaced. Find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.

If...	Then...
alternating **E** and **0** and **1**	No NVMs are detected on the LNW2 SYSCTL. Install two Alcatel-Lucent-supplied NVMs in the LNW2 or find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
alternating **E** and **0** and **2**	NVMs are present but not readable. Check to make sure they are properly seated and repeat this procedure.
alternating **E** and **0** and **3**	Not Supported. Find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
alternating **E** and **1** and **0**	LNW2 SYSCTL does not boot. No compatible generic on the NVMs in the LNW2 SYSCTL. Find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure or contact your next level of support.
Letter **F**	LNW2 SYSCTL faceplate latches are not fully seated. Unseat the LNW2 SYSCTL and repeat this procedure, properly seating the faceplate latch.
alternating **N** and **O** and **x**	"x" indicates that the NVM socket (1 or 2) is empty or the NVM installed is failed. Replace the indicated NVM or find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
Letter **U**	LNW2 SYSCTL does not boot due to unexpected or unreadable shelf type. Repair the problem generally caused by bent pins and repeat this procedure.
flashing **b**	Boot in progress.

If...	Then...
A red, four-segment square (2 x 2) appears in the **IND** display on the LNW2 SYSCTL.	Acknowledges the **UPD/INIT** button was momentarily pushed. Pushing the **UPD/INIT** button while in Maintenance Mode has no effect.

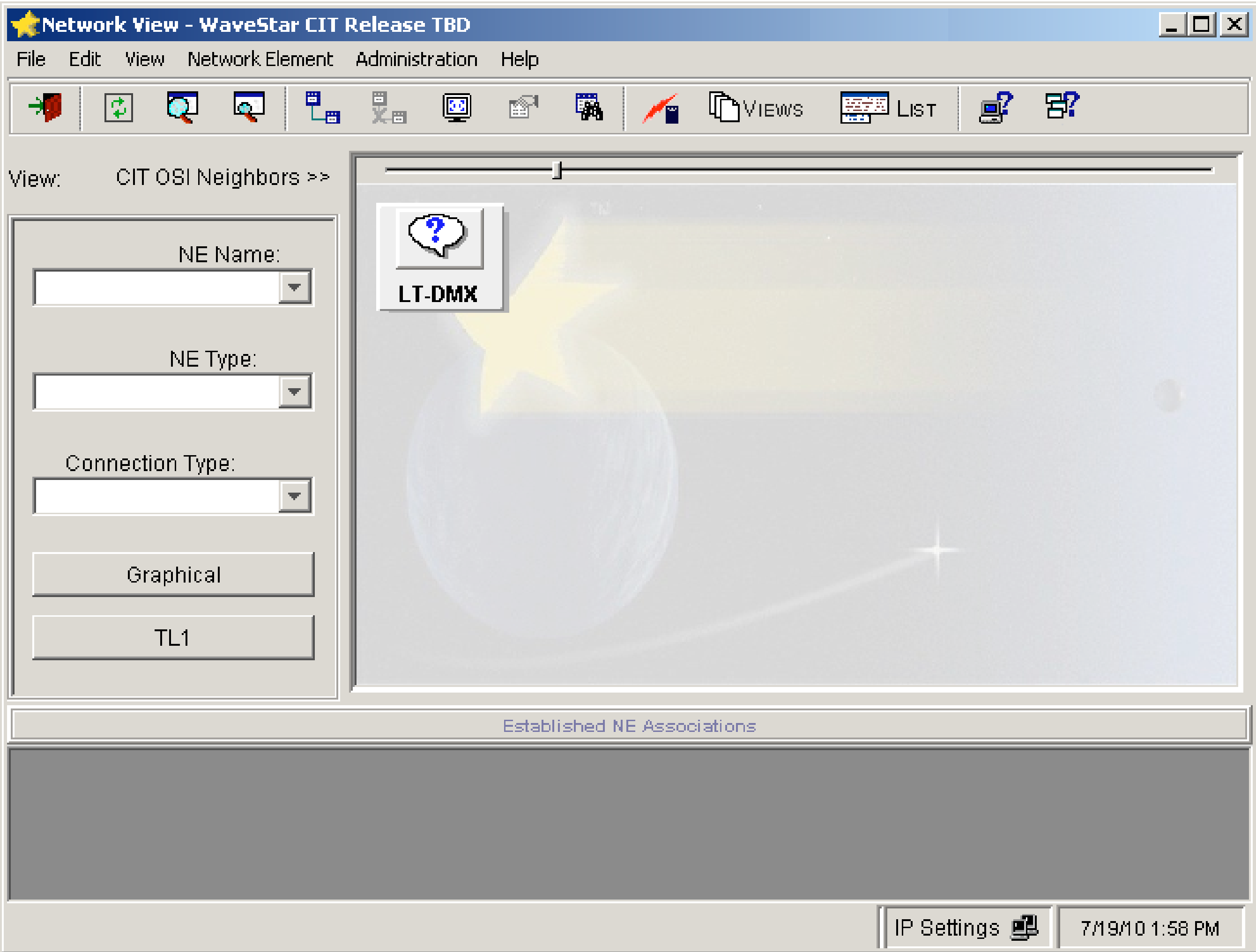
13 Connect the cross-over LAN cable from the Network Interface Card (NIC) on the PC to the rear **J16 IAO LAN** port on the Alcatel-Lucent 1665 DMX shelf backplane or the front **LAN** port on the LNW2 SYSCTL circuit pack faceplate. (When TCP/IP is enabled on the rear LAN port, OSI is disabled.)

14 From the Network View of the *WaveStar*® CIT session you established in Procedure 6-17: “Upgrade software generic via FTP” (p. 6-175), select the **View:** pull-down menu and select **CIT OSI Neighbors**.

Important! This **View:** is not the menu bar item View → ...; it is located above the NE Name pull-down menu.

Result: The CIT OSI Neighbor(s) are automatically detected.

If you were previously logged in to the NE and/or you do not see your NE, from the Network View, select **View** → **Refresh OSI View**.



15 In the Network View, right-click the LT-DMX NE icon that was detected, and select **Graphical Using** → **OSI** from the resulting menu.

Result: The *System Type Selection* window appears.

16 In the *System Type Selection* window, select DMX and click **OK**.

Result: The *NE Login Dialog* window appears.

17 **Important!** Because the shelf is in Maintenance Mode, your logins and passwords are default.

Enter the following in the *NE Login Dialog* window (login information is case sensitive) to log in to the NE:

User ID: ***LUC01***

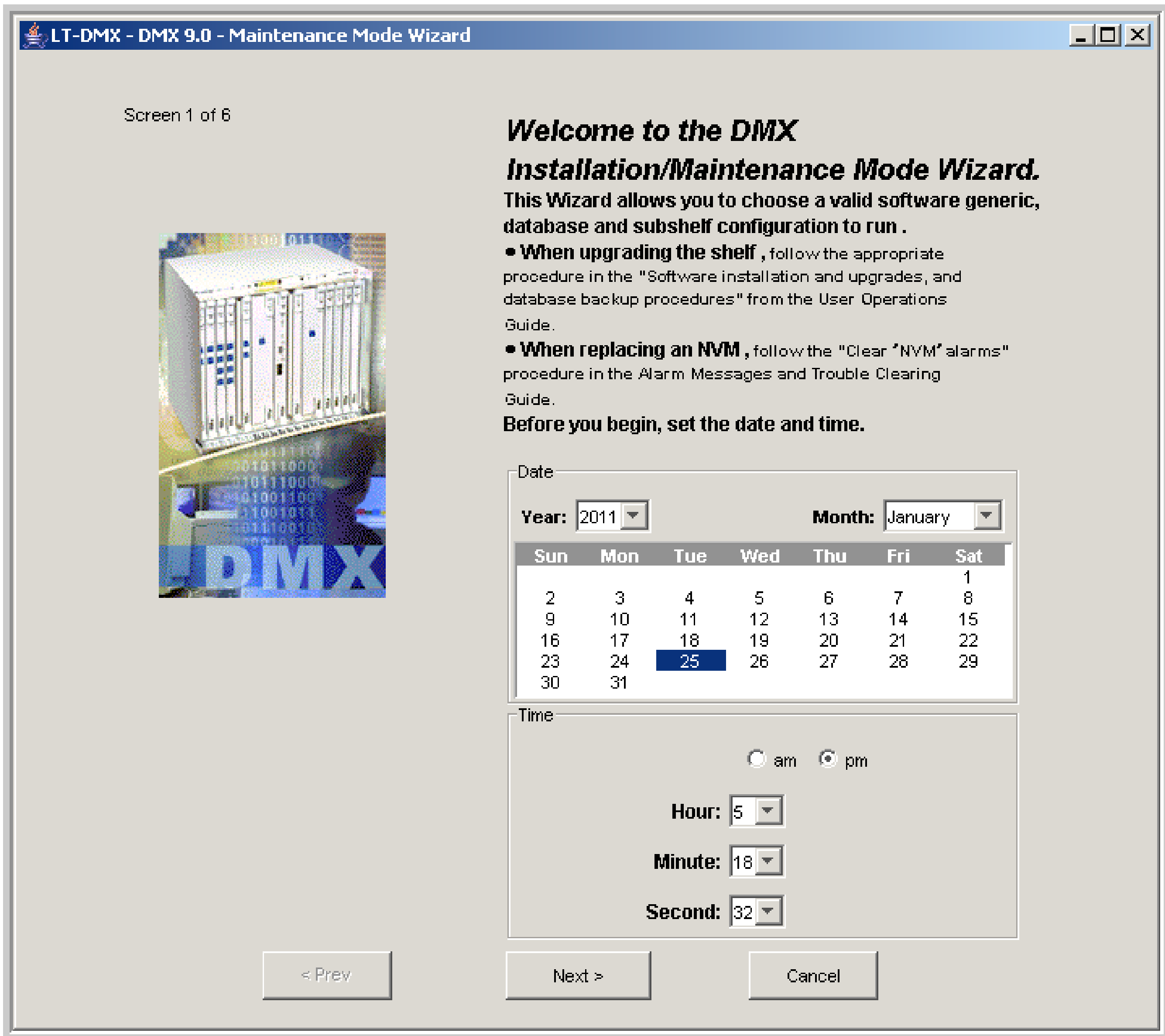
Password: ***DMX2.5G10G***

Click **OK**.

Important! After you select your backup database, complete the Maintenance Mode Wizard, and the NE restarts, your original User IDs and Passwords are restored.

Result: Screen 1 of 6 in the Maintenance Mode Wizard appears.

Depending on the boot code of your SYSCTL (refer to Step 12), the title bar of the Maintenance Mode Wizard displays either DMX 6.0, DMX 7.0, DMX 7.1, DMX 8.0, DMX 9.0, or DMX 9.1



This screen picks up the time format preference from the *WaveStar*® CIT.

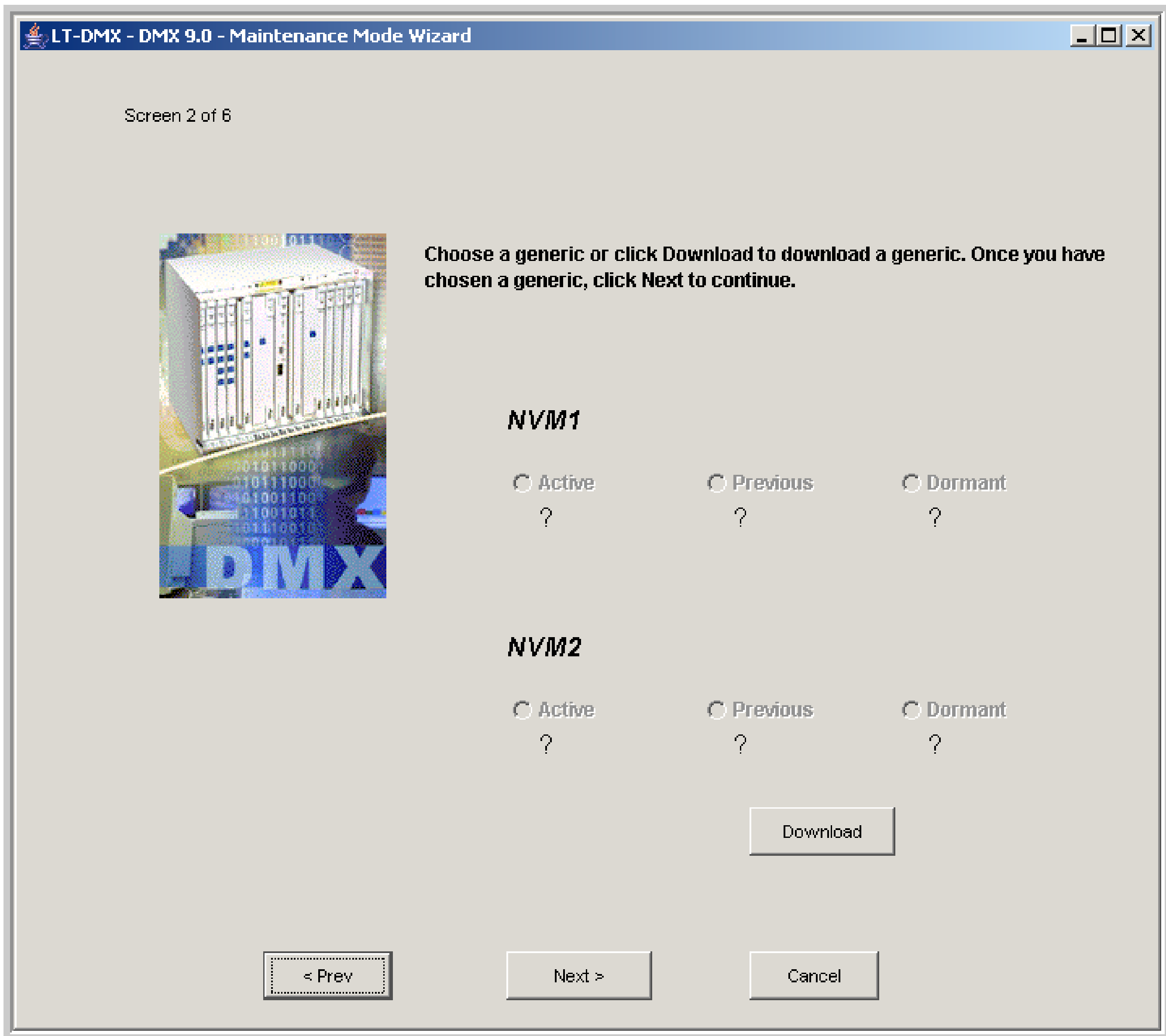
You can provision the time format display for your *WaveStar*® CIT from the Network View by selecting **View** → **Preferences** and clicking the Display tab. This screen allows you to choose your preference for time format, either a 12-hour clock or a 24-hour clock.

- If your time format preference is a 12-hour clock, from the **Time** panel, select **Hour:** (0–12), **Minute:** (0–59), and **Second:** (0–59) from the pull-down menus. You must also specify am or pm by selecting one of the radio buttons.
- If your time format preference is a 24-hour clock, From the **Time** panel, select the **Hour:** (0–23), **Minute:** (0–59), and **Second:** (0–59) from the pull-down menus.

18 **Important!** The actual time and date are preset from your PC.

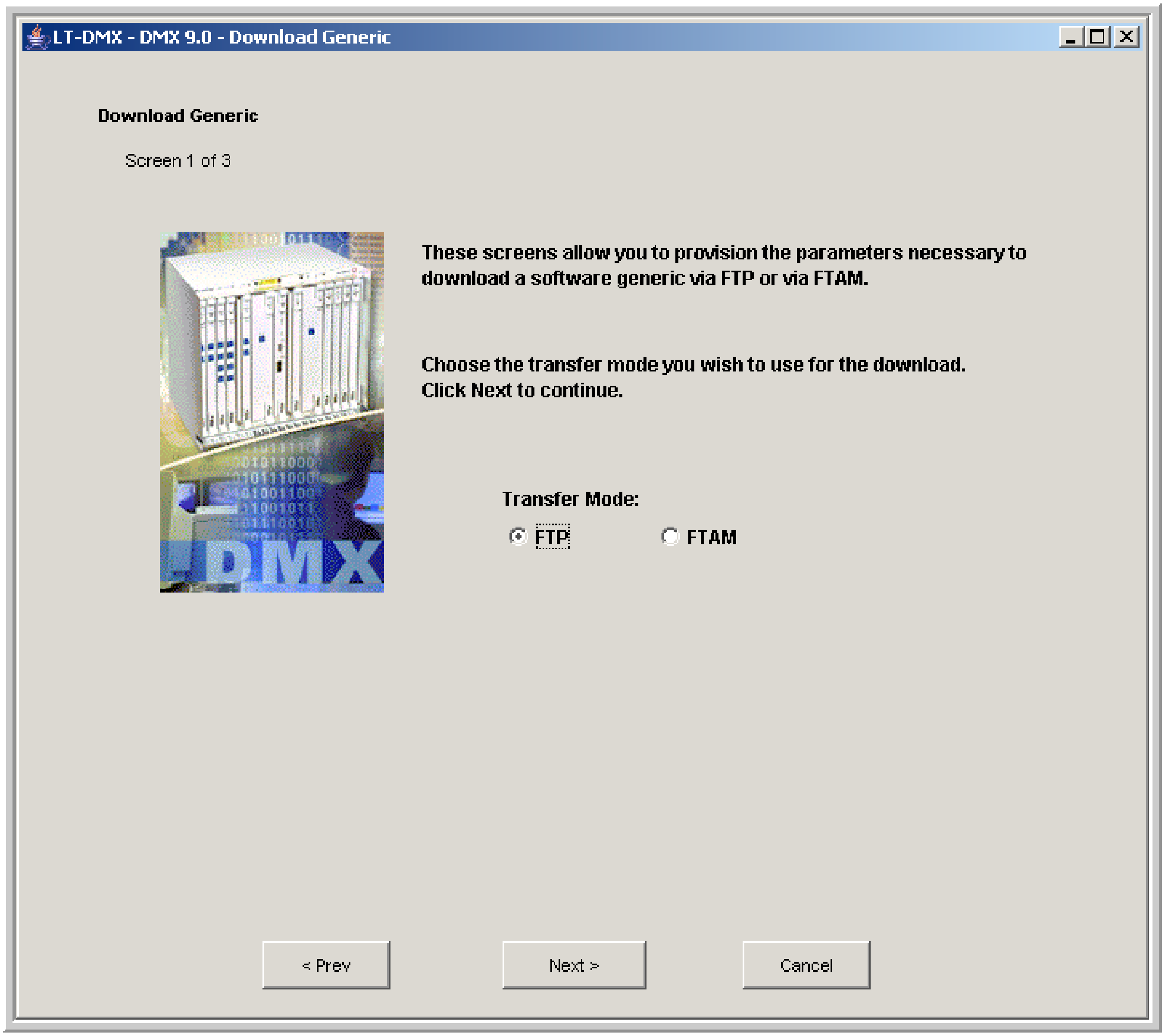
On Screen 1 of 6 in the Maintenance Mode Wizard, read the information, verify the date and time, make any required changes, and click **Next**.

Result: Screen 2 of 6 in the Maintenance Mode Wizard appears.



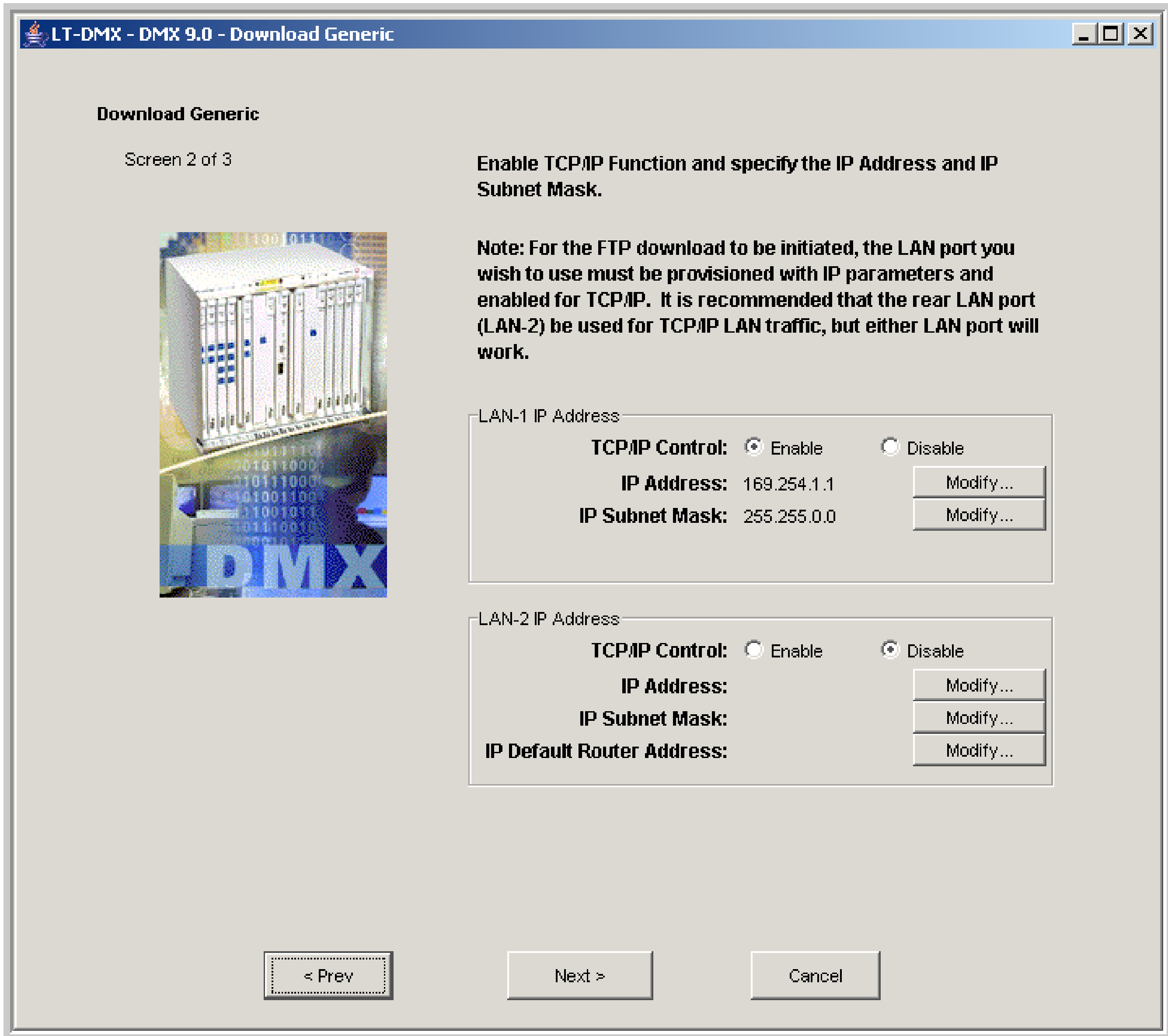
19 On Screen 2 of 6 in the Maintenance Mode Wizard, click **Download**.

Result: Screen 1 of 3 in the Download Generic Wizard appears.



20 On Screen 1 of 3 in the Download Generic Wizard, read the information, select **FTP** and click **Next**.

Result: Screen 2 of 3 in the Download Generic Wizard appears.

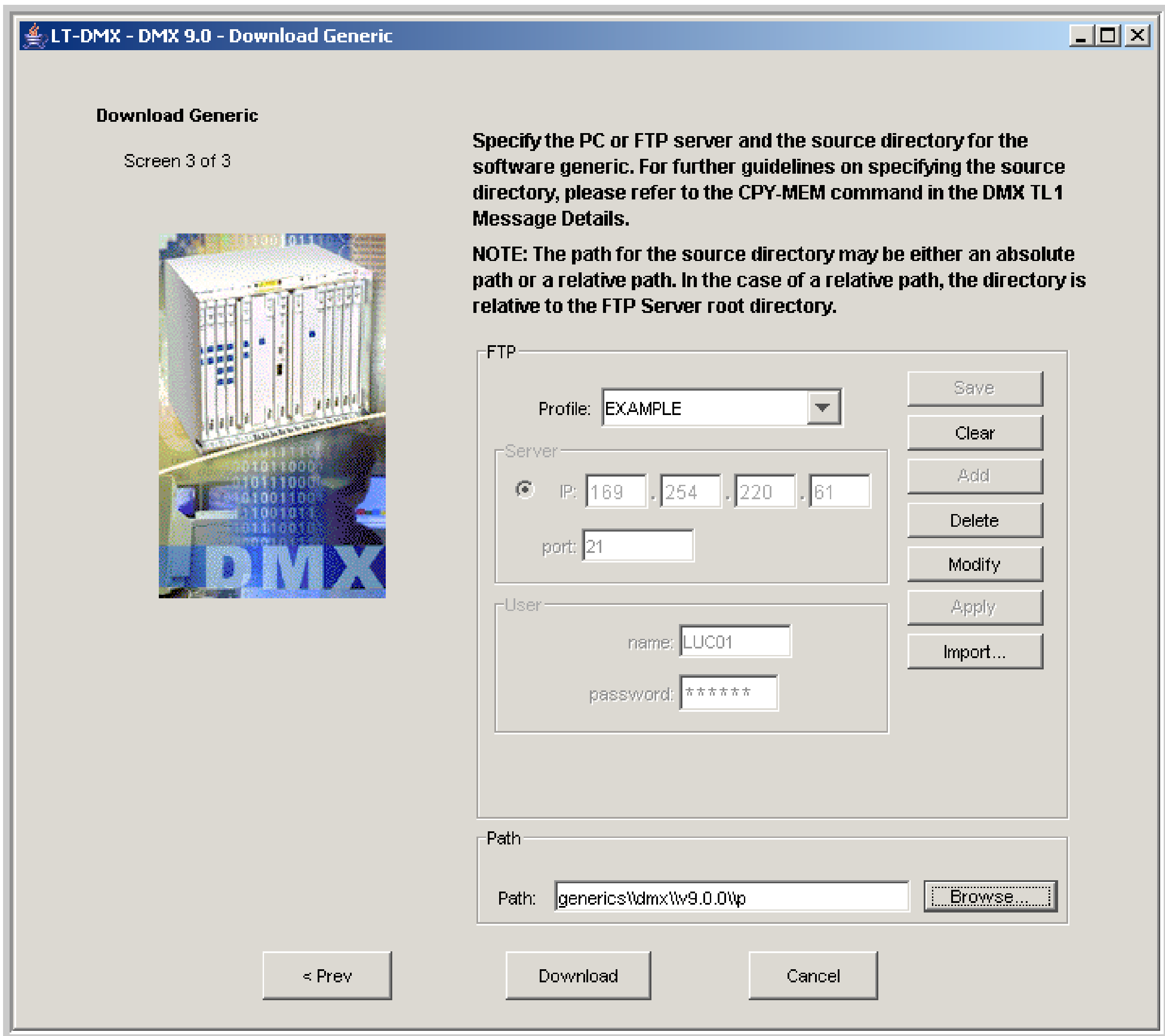


21 **Important!** LAN-1 is the **LAN** port on the faceplate of the LNW2 SYSCTL circuit pack. LAN-2 is the **J16 IAO LAN** port on the rear of the Alcatel-Lucent 1665 DMX shelf.

If the boot code of your LNW2 (Step 12) was 7.1 or later, you may see the IP Address and IP Subnet Mask field populated with the defaults illustrated in Screen 2 of 3. Changing anything on this screen will cause the shelf to reset.

If required, follow the instructions to enable TCP/IP Control on the LAN port to which you are connected. Click **Modify** to enter the IP Address, IP Subnet Mask, and/or IP Default Router Address. Click **Next**.

Result: Screen 3 of 3 in the Download Generic Wizard appears.



22 Select the connection from the **Profile** pull-down menu and proceed to Step 24. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user ID/password can be different.)

23 If you entered connection information in Step 22 and wish to keep the information for future FTP activities:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

Important! Entries to the **Profile** pull-down menu can be changed using the **Modify**, **Apply**, and **Save** buttons or removed using the **Delete** button.

24 On Screen 3 of 3 in the Download Generic Wizard in the **Path** panel, enter the current location of the generic to be downloaded in the Path field or use the **Browse** button to select the generic to be downloaded. (If the FTP server is not the local host, the **Browse** button is greyed out.) Click **Download**.

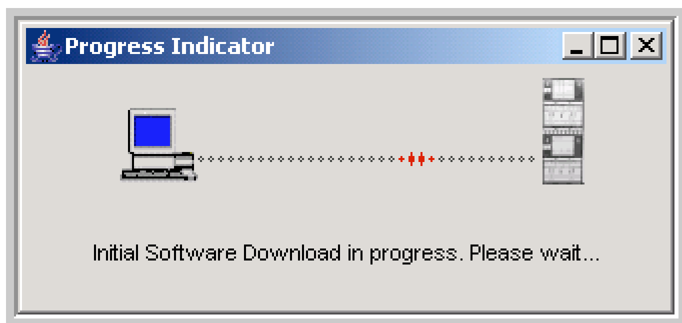
The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: `C:\Program Files\Alcatel-Lucent\WaveStar CIT\generics\DMX\9.1.x\p`. If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.The syntax of the relative path must start with the path name; for example: **`\generics\DMX\9.1.x\p`**. If necessary, replace 9.1.0 with your current release, for example 9.1.1.

If the FTP server is not the *WaveStar*® CIT, then enter the path starting at the FTP home directory on the server.

Result: A warning message appears listing the options you provisioned in the previous screens.

25 Verify the information and either click **Yes** to start the download process or click **No** to return to the download screen and change your selections.

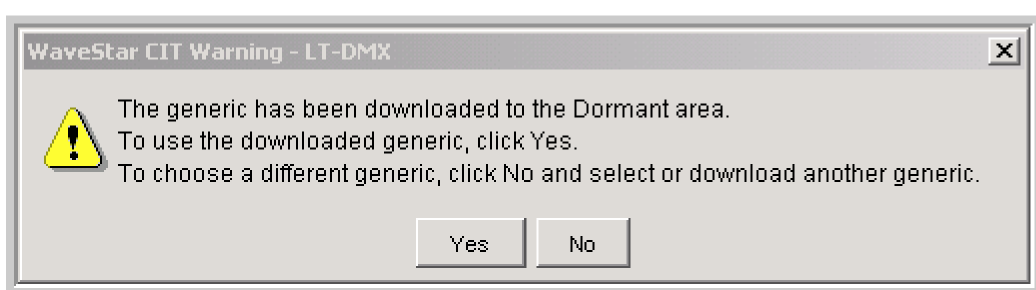
Result: If you choose yes, the following initial software download progress indicator runs for approximately 30 minutes.



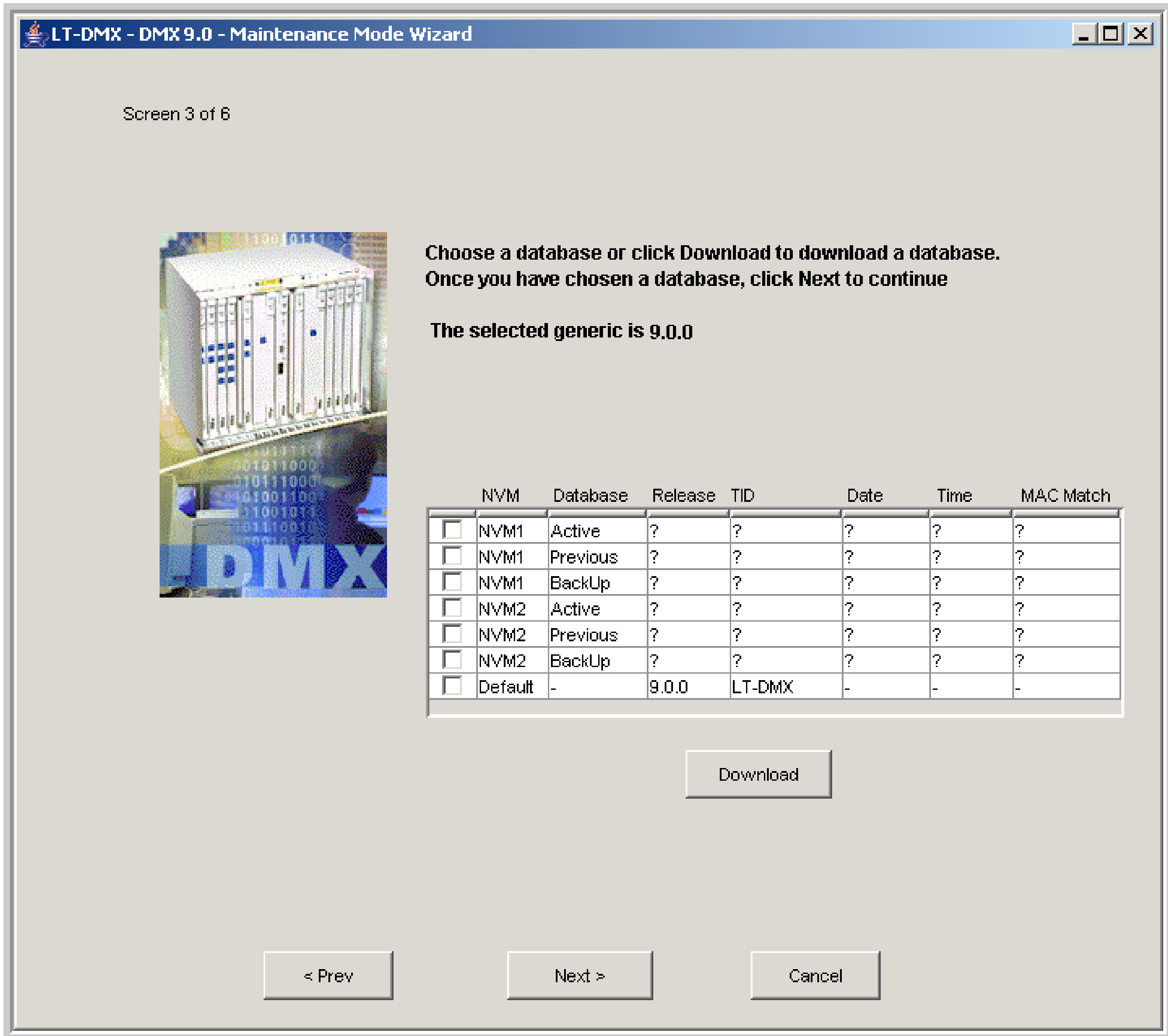
26 Do you wish to observe the FTP download progress?

If...	Then...
Yes	Proceed to Procedure 6-24: "Observe FTP progress" (p. 6-285) and then continue with Step 27.
No	Continue with Step 27.

27 Once the software generic download is complete, the following confirmation message appears. Click **Yes** to use the generic that is now in the Dormant area.



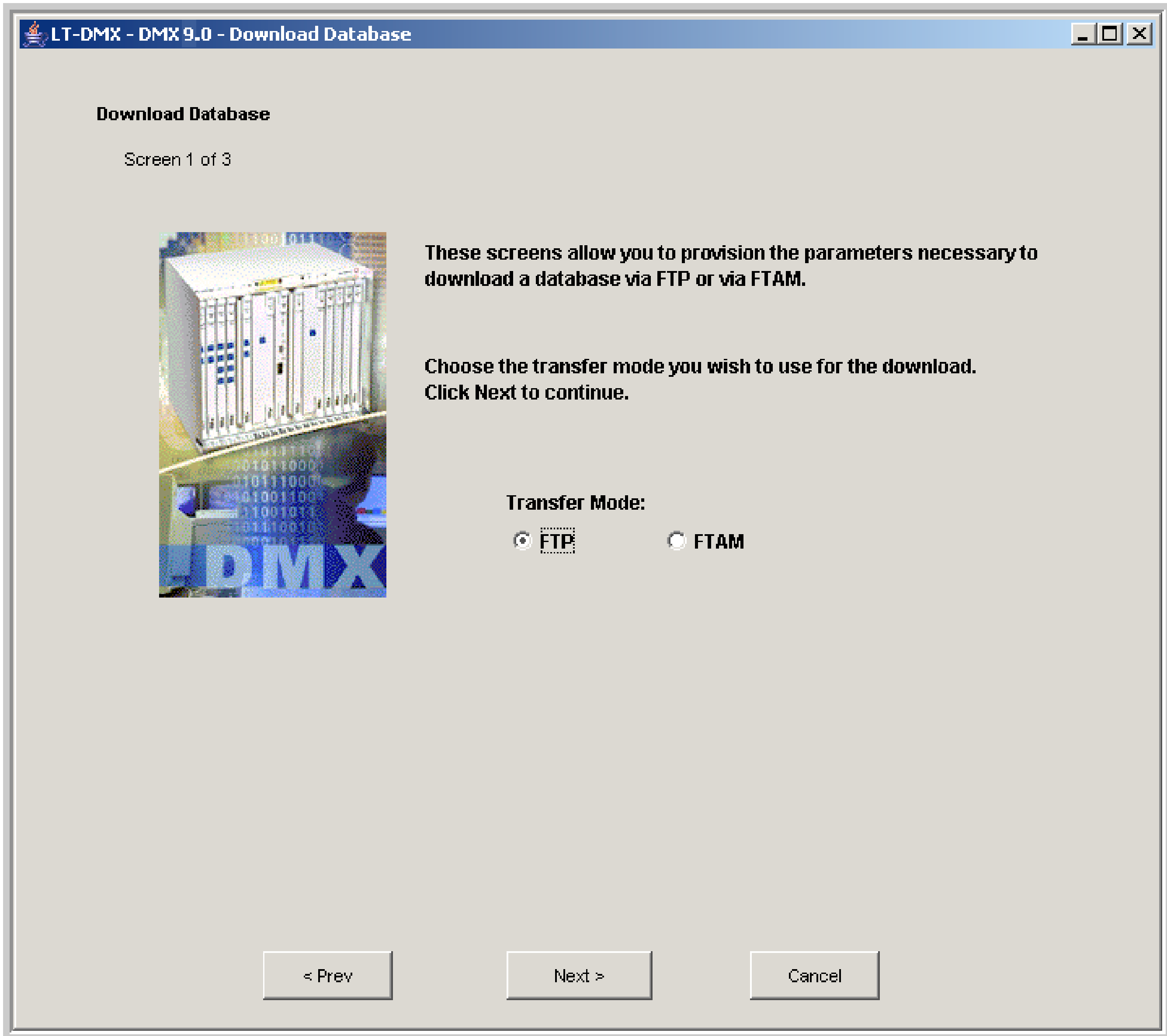
Result: Screen 3 of 6 in the Maintenance Mode Wizard appears.



28 **Important!** Do NOT select the default database or you could loose service to your shelf. You MUST download your previously backed up database.

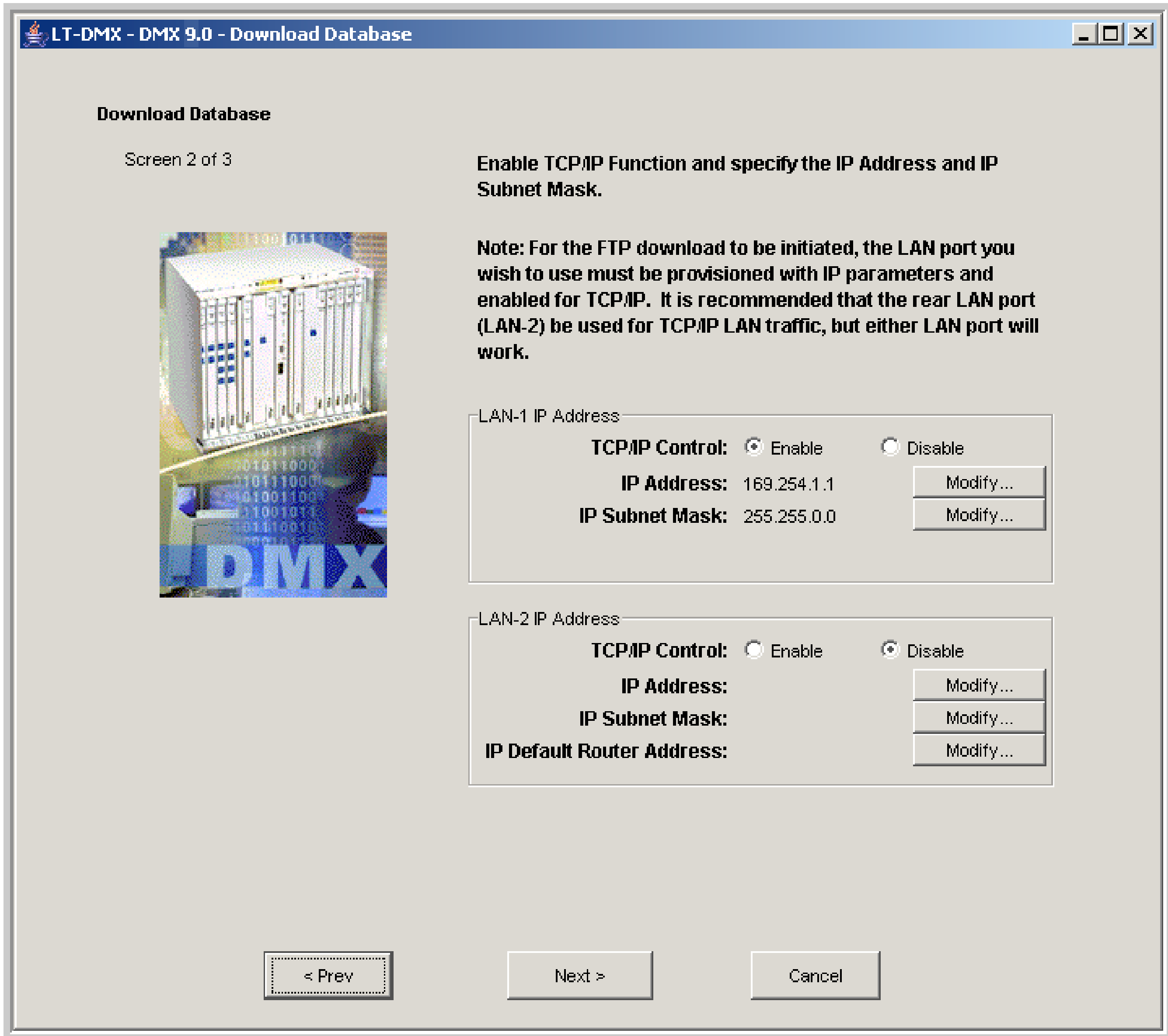
On Screen 3 of 6 in the Maintenance Mode Wizard, click **Download**.

Result: Screen 1 of 3 in the Download Database Wizard appears.



29 On Screen 1 of 3 in the Download Database Wizard, read the information, select **FTP** and click **Next**.

Result: Screen 2 of 3 in the Download Database Wizard appears.

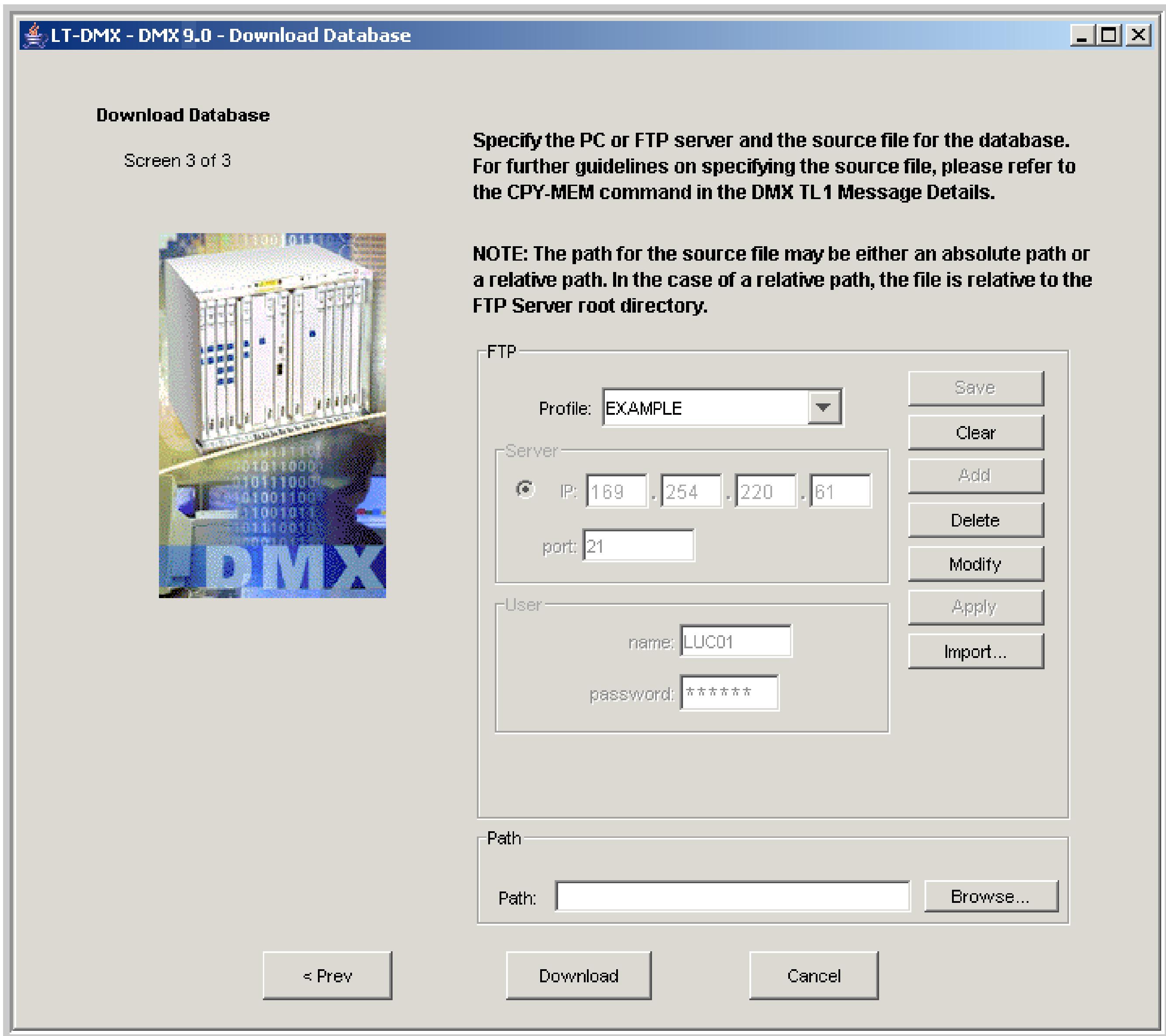


30 **Important!** LAN-1 is the **LAN** port on the faceplate of the LNW2 SYSCTL circuit pack. LAN-2 is the **J16 IAO LAN** port on the rear of the Alcatel-Lucent 1665 DMX shelf.

On Screen 2 of 3 in the Download Database Wizard, the information entered in Step 21 is still present and valid. If the information is not present, follow the instructions to enable TCP/IP Control on the LAN port to which you are connected. Click **Modify** to enter the IP Address, IP Subnet Mask, and/or IP Default Router Address.

Click **Next**.

Result: Screen 3 of 3 in the Download Database Wizard appears.



31 Select the connection from the **Profile** pull-down menu and proceed to Step 33. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user ID/password can be different.)

32 If you entered connection information in Step 31 and wish to keep the information for future FTP activities:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

Important! Entries to the **Profile** pull-down menu can be changed using the **Modify**, **Apply**, and **Save** buttons or removed using the **Delete** button.

33 On Screen 3 of 3 in the Download Database Wizard in the **Path** panel, enter the location where the database information is stored. Enter the path and filename exactly as it was entered in Step 5. For example: **`\backups\<subdirectory>\<filename>`**.

You can also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and over-write the default entry. The **Browse** button is not available (greyed out) if the FTP server is not the local *WaveStar*® CIT or the IP address of the FTP server is not in the same subnet as the IP address of the shelf.

Click **Download**.

Important! The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.

The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is

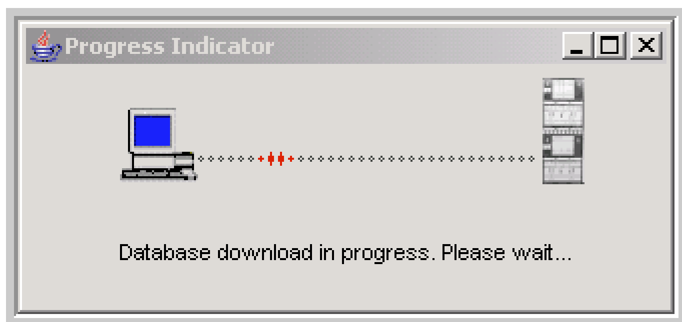
```
C:\Program Files\Alcatel-Lucent\WaveStar CIT\
```

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.

Result: A warning message appears listing the options you provisioned in the previous screens.

34 Verify the information and click **Yes**.

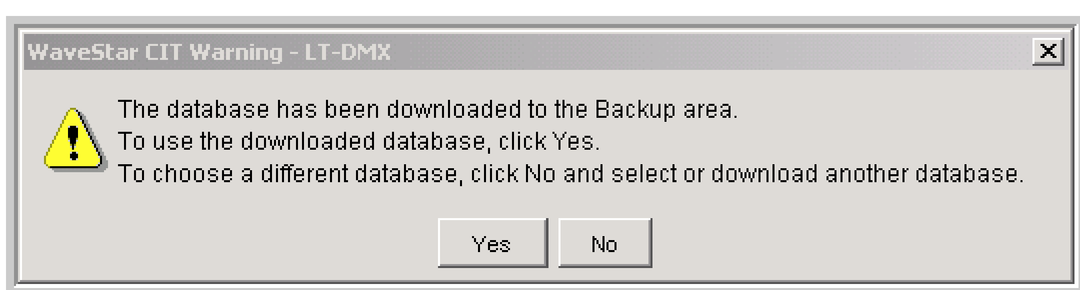
Result: If you choose Yes, the database download progress indicator runs for approximately two minutes.



35 Do you wish to observe the FTP download progress?

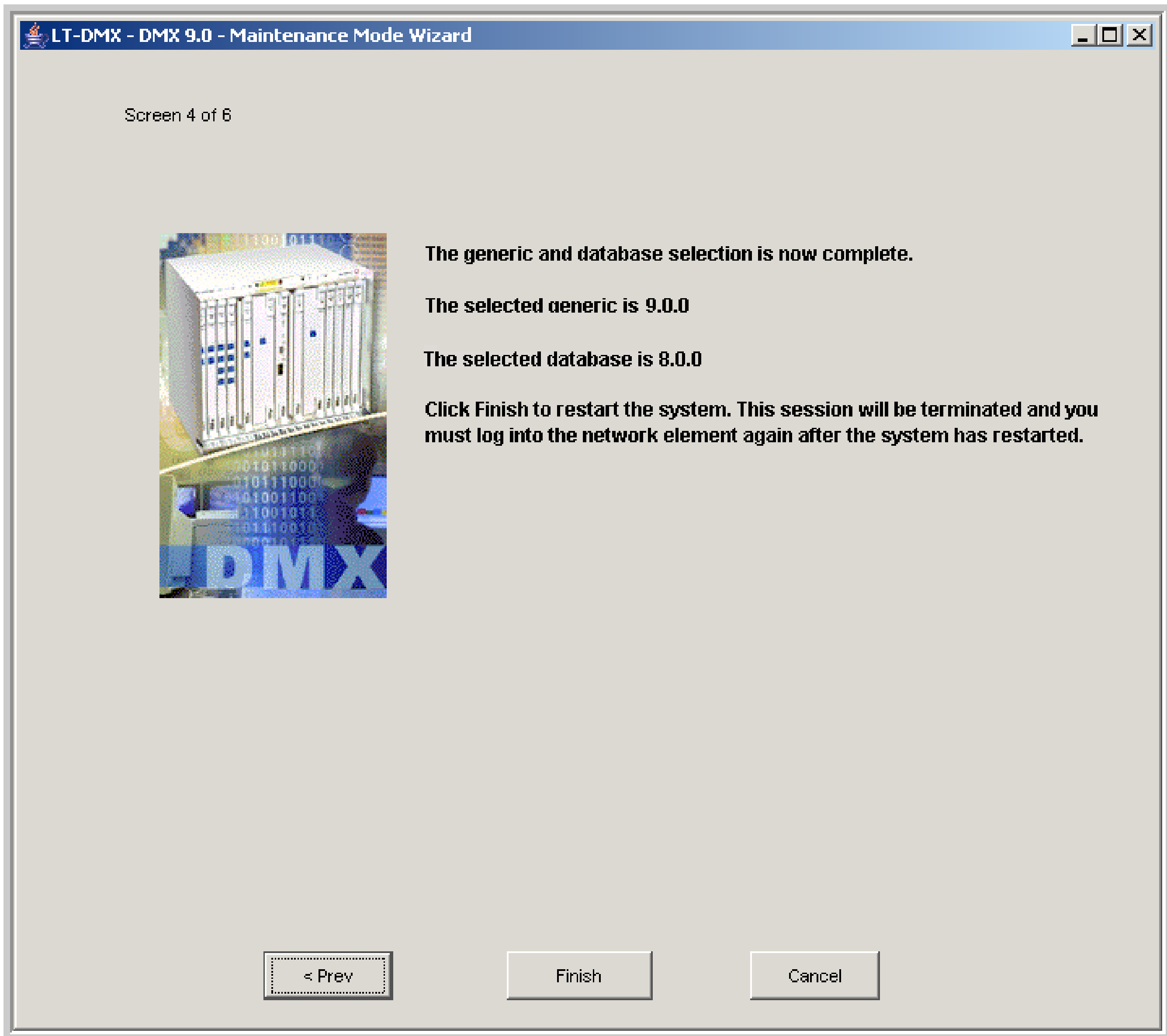
If...	Then...
Yes	Proceed to Procedure 6-24: "Observe FTP progress" (p. 6-285) and then continue with Step 36.
No	Continue with Step 36.

36 Once the database download is complete, the following confirmation message appears. Click **Yes** to use the database that is now in the Backup area.



Result: Screen 6 of 6 in the Maintenance Mode Wizard appears. In this screen, 9.1.0 is an example; your selected generic could be different, for example 9.1.1.

5.1.3 is an example too; your selected database could be 5.1.x.



37 On Screen 6 of 6 in the Maintenance Mode Wizard, read the information, verify that you have selected the correct generic and database, and click **Finish** to restart the system and apply the generic and database.

Result: The Maintenance Mode Wizard closes and your connection to the shelf is terminated.

The LNW2 SYSCTL exhibits the following visible cycles while the generic and database are installed and validated and the SYSCTL reboots:

1. For approximately 12 minutes, the alternating **M** and **P** and **X** (X represents 6, 7, 8, or 9, depending on your Maintenance Mode) and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **Y** (Y represents 0 or 1, depending on your Maintenance Mode) continue to appear in the **IND** display on the SYSCTL.
2. After approximately 12 minutes, all LEDs extinguish and the **IND** display on the SYSCTL is blank for approximately 5 seconds.
3. A flashing **b** appears in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 60 seconds and the **IND** display is blank for approximately 20 seconds.
4. The **ACTIVE** LED lights and remains lighted.
5. A flashing **b** appears again in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 2.5 minutes while the database is being converted and the **IND** display is blank.
6. When nothing appears in the **IND** display and the **ACTIVE** LED is lighted and the other LEDs return to their previous state (pre-LNW1 backup), the NE software and database installation is complete.

   However, smart circuit packs can be upgrading their firmware. If flashing green **ACTIVE** LEDs are present on a circuit pack, firmware is currently being downloaded to that pack. Wait until all smart circuit packs finish upgrading their firmware before proceeding.

   If an alarm condition existed before the upgrade, the NE rediscovers the alarm condition and activates the appropriate LEDs on the shelf.
7. Continue with Step 38.

---

38 To verify that the upgrade was successful, depress and hold the **ACO TEST** push-button on the LNW2 SYSCTL for about 4 seconds.

Result: All LEDs on the shelf light. A red, 35-segment (5 x 7) rectangle appears in the **IND** display on the SYSCTL. Since the **IND** display is a 35-segment display, this test indicates all segments are working.

---

39 Release the **ACO TEST** push-button on the LNW2 SYSCTL when the red rectangle disappears in the **IND** display.

Result: The current software generic appears in the **IND** display on the LNW2 SYSCTL and the shelf LEDs return to their previous status.

---

40 From the Network View of the *WaveStar*® CIT session you established in Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175), select the **View:** pull-down menu and select **CIT OSI Neighbors**.

Important! This **View:** is not the menu bar item View → ...; it is located above the NE Name pull-down menu.

---

41 From the Network View, select **View** → **Refresh OSI View**.

Result: The CIT OSI neighbor(s) are automatically detected.

Your TID is your original TID, the same TID provisioned on your 5.1.x NE.

---

42 In the Network View, right-click the NE icon that was detected, and select **Graphical Using** → **OSI** from the resulting menu.

Result: The *System Type Selection* window appears.

---

43 In the *System Type Selection* window, select DMX and click **OK**.

Result: The *NE Login Dialog* window appears.

---

44 In the NE login window, login to the shelf using your original user ID and password; the same user ID and password provisioned on your 5.1.x NE.

Click **OK**.

Result: The title bar of the System View and the legal notice text both reflect the current NE software generic, for example: 9.1.0.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

---

45 Is the Generic Software Version correct?

If...	Then...
Yes	STOP! End of Procedure.
No	Contact your next level of support.

END OF STEPS

Procedure 6-17.3: Upgrade software generic via FTP (7.1.x, 8.0.x, 9.0.1 or later to 9.1.x)

Overview

Use this procedure to download the software generic via the FTP from the *WaveStar*® CIT to the local network element. To download the software generic to a local shelf via FTP, refer to Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175). To download the software generic to a remote shelf via FTTD, refer to Procedure 6-18: "Upgrade software generic via FTTD" (p. 6-212).

> **Important!** Your NE must be running Release 7.1.x, 8.0.x, or 9.0.1 or later to use this procedure.

Required equipment

Refer to "Required equipment" (p. 6-175) in Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure, complete Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175).

Steps

Complete the following steps to download and upgrade system software via FTP.

---

1 Before upgrading the network, perform a backup the NE database.

> **Reference:** Procedure 6-21: "Backup and restore NE database via FTP" (p. 6-252)

---

2 From the System View menu, select **Administration** → **View NE Administration**. Verify that *File Transfer Protocol (FTP)* is Enabled and click **Close**.

---

3 If necessary, select **Administration** → **Set NE** and enable **File Transfer Protocol**. Click **OK**.

---

4 Provision the destination shelf for TCP/IP communications. From the System View menu, select **Administration** → **Data Communications**.

Result: The *Data Communications* window appears.

5 Which port are you provisioning for TCP/IP?

If...	Then...
LAN-1 for the front **LAN** port on the SYSCTL (LAN-1 is intended to be used for local [direct] software downloads.)	Continue with Step 6.
LAN-2 for the rear **J16 IAO LAN** port on the backplane	Proceed to Step 7.

6 From the *Data Communications* window, click the **TCP/IP** tab and provision the following fields accordingly for LAN-1:

1. **Port AID:** select the port that you are using for FTP: LAN-1
2. **TCP/IP Function:** select Enable
3. Click **Modify** to either enter or change the following:
   - IP Address
   - IP Subnet Mask
   - IP Default Router Address (Because LAN-1 is intended to be used for local [direct] software downloads, the IP Default Router Address is not required when using LAN-1).
4. Proceed to Step 8.

7 From the *Data Communications* window, click the **TCP/IP** tab and provision the following fields accordingly for LAN-2:

1. **Port AID:** select the port that you are using for FTP: LAN-2
2. **TCP/IP Function:** select Enable
3. Click **Modify** to either enter or change the following:
   - IP Address
   - IP Subnet Mask
   - IP Default Router Address

8 Click **Apply**.

Important! If the TCP/IP information for one of the LAN ports is already provisioned, then reprovisioning that port, or provisioning the other LAN port can cause the shelf to reset.

Result: A warning message appears.

9 Click **Yes** and then click **Close** on the *Data Communications* window.

10 Specifying either OSI or Serial in the **Connection Type:** field, log in to the destination shelf again.

11 From the System View menu, select **Configuration** → **Software** → **Download Software**.

Result: The *Download Software* window appears.

12 In the pull-down **Download From/Via:** menu, select **FTP**. Select the connection from the **Profile** pull-down menu and proceed to Step 14. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user ID/password can be different.)

13 If you entered connection information in Step 12 and wish to keep the information for future FTP activities:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

Important! Entries to the **Profile** pull-down menu can be changed using the **Modify**, **Apply**, and **Save** buttons or removed using the **Delete** button.

14 In the **Source/Destination Directory Path** panel, enter the current location of the generic to be downloaded or use the **Browse** button (if available) to select the generic to be downloaded. If the FTP server is either undefined or not the local host, the **Browse** button is greyed out.

Important! If you selected the default installation location for the *WaveStar®* CIT and software generic: **`\generics\DMX\9.1.x\p`**. If necessary, replace 9.1.0 with your current release, for example 9.1.1.

The value of the Path field can be either an absolute path or a relative path that is relative to the root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: `C:\Program Files\Alcatel-Lucent\WaveStar CIT\generics\DMX\9.1.x\p`. If you had an older *WaveStar®* CIT installed prior to installing the current *WaveStar®* CIT, your path could start with C:\Program Files\Lucent Technologies\. If necessary, replace 9.1.0 with your current release, for example 9.1.1.The syntax of the relative path must start with the path name; for example: **`\generics\DMX\9.1.x\p`**. If necessary, replace 9.1.0 with your current release, for example 9.1.1.

15 In the **Product Type** panel, select the product type of the software generic that you are downloading (not necessarily the same as the NE to which you are downloading).

16 Click **OK**.

Result: A warning message appears asking you to confirm executing this command. Verify the information and click **Yes**. While the download is in progress, a progress indicator window is present.

The download takes approximately 30 minutes.

The download can be cancelled any time by pressing the **Cancel** button on the progress screen.

When the transfer is complete, the *Progress Indicator* window closes and the download software successful window appears. Click **OK**.

17 Is the *WaveStar®* CIT your FTP server and do you wish to observe the FTP download progress?

If...	Then...
Yes	Proceed to Procedure 6-24: "Observe FTP progress" (p. 6-285) and then continue with Step 18.

If...	Then...
No	Continue with Step 18.

18 **Important!** Do NOT insert a new circuit pack in the shelf until after you apply the new software generic and clear the `dormant/exec version mismatch` condition.

Do you wish to apply (activate) the software generic that you recently downloaded to the dormant area of the Alcatel-Lucent 1665 DMX shelf?

If...	Then...
Yes	Proceed to Procedure 6-20: "Apply software generic" (p. 6-249) and then continue with Step 19.
No	Continue with Step 19.

19 Do you wish to upgrade additional shelves via FTP?

If...	Then...
Yes	Repeat this procedure from Step 2 for each shelf that you wish to upgrade via FTP.
No	STOP! End of Procedure.

END OF STEPS

Procedure 6-18: Upgrade software generic via FTTD

Overview

Use this procedure to download the software generic to a shelf without TCP/IP connectivity via FTTD (FTAM-FTP gateway).

Note: You can upgrade directly to 9.1.x from the following releases:

- R5.1.3/5.1.7
- R7.1.2
- R8.0.2/R8.0.3/8.0.4/8.0.5/8.0.6
- R9.0.1

You must complete a two-step upgrade to 9.1.x from the following releases:

- R6.0.1/6.0.2/6.0.4 through R8.0.5
- R7.0.2 through R8.0.5
- R7.1.1/7.1.4 through R8.0.6

You must complete a three-step upgrade to 9.1.x from R5.1.4/5.1.5 through R7.0.2, and then through R8.0.5.

To download the software generic to a local shelf using SFTP, refer to Procedure 6-16: "Ugrade software generic via SFTP" (p. 6-171).

To download the software generic to a local or remote shelf via FTAM, refer to Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218).

To download the software generic to a local shelf via FTP, refer to Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175).

Important! Your NE must be running Release 7.0.2, 7.1.x, 8.0.x, or 9.0.1 to use this procedure.

Privilege level

You must log in as a Privileged user to complete this procedure.

Required equipment

In addition to "Required equipment" (p. 6-3) listed in this chapter, the following equipment is also required:

- CAT5 Ethernet cable with either a 10/100 hub or a cross-over cable for the **LAN** or **IAO LAN** port
- Copy of the new system generic software program on your PC or FTP server
- Current *Alcatel-Lucent 1665 Data Multiplexer (DMX) Software Release Description* for the software generic being installed

Important! If the FTP server fails to start, it could mean that another program using an FTP server is already running. Depending on what operating system you are using, you must go to the device file and disable the FTP server. Refer to Procedure 6-25: "Disable an FTP server on your PC" (p. 6-287) for instructions for each allowed operating system.

Before you begin

Before performing this procedure:

1. Refer to "Before you begin" (p. 6-3) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
2. Verify that new software generic program is available.
3. Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Software Release Description* for a description of any special considerations required when installing this version of software.

This procedure uses FTP (file transfer protocol) and FTAM-FTP gateway/file transfer translation device (FTTD) to download software to a shelf. FTTD allows Alcatel-Lucent 1665 DMX to function as a gateway network element (GNE) that facilitates file downloads between FTP servers and remote network elements (RNEs) connected to the Alcatel-Lucent 1665 DMX.

Important! If you log in via TCP/IP, your PC must be part of the GNE's TCP/IP Gateway Host List. Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* for more information.

Steps

Complete the following steps to download system software via FTTD.

---

1 Connect the PC and establish a *WaveStar*® CIT session to the gateway Network Element.

Important! You must login via either OSI or TCP/IP.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

---

2 From the System View menu, select **Administration** → **Set NE** and enable **File Transfer Protocol (FTP)** and **FTAM-FTP (FTTD) Gateway Control**.

---

3 Click **OK**.

4 Is your remote NE in the same OSI network as your gateway NE?

If	Then
Yes	Proceed to Step 6.
No	Continue with Step 5.

5 From the System View, select **Administration** → **Data Communications**.

Select the **Network Layer** tab and record the NSAP from the **Network Service Access Point** panel (the NSAP is a 40-digit hex number). This NSAP is required later in this procedure.

6 Establish a *WaveStar*® CIT session to the remote Network Element to which you wish to download the NE software generic.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

7 Before upgrading the network, perform a backup the NE database.

Reference: Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264)

8 From the System View menu, select **Configuration** → **Software** → **Download Software**.

Result: The *Download Software* window appears.

9 In the pull-down **Download From/Via:** menu, select **FTTD** and verify that the **FTTD** tab is selected.

10 Define the FTAM-FTP Gateway in one of the following ways:

- If the TID of the FTAM-FTP Gateway has been previously defined, select it from the **TID** pull-down menu.

OR

- If the gateway NE and the remote NE are in the same OSI area:
  1. Enter the TID of the FTAM-FTP Gateway in the **TID** field and click **Get NSAP**. (If any fields on this screen are populated, click **Clear** before you enter the TID.)
  2. Click **Add** and then **Save**. The TID is added to the pull-down menu for this CIT. If you replace the SYSCTL in the GNE, re-enter the NSAP address for this gateway NE's TID.

  OR
- If the gateway NE and the remote NE are *not* in the same OSI area:
  1. In the **FTTD** panel, select **_template_** from the **TID:** pull-down, which pre-populates most of the fields on this form (required value for **Psel** is 02, **Ssel** is 5353, and **Tsel** is 5454).
  2. Click **Modify**.
  3. Replace **_template_** with the TID of the FTAM-FTP gateway.
  4. Complete the NSAP Address panel with the NSAP of the FTTD gateway recorded in Step 5.

     In most cases, you only need to replace the System Identifier (**Sys:**) field with the Mac Address of the FTTD gateway.

     Note: The Mac Address is the first 12 digits of the last 14 digits of the NSAP. The Mac Address of Alcatel-Lucent products begin with “00601D”.

     Example: The Mac Address for NSAP Address 39840F80000000000000000000 00601D2CBC1800 is 00601D2CBC18.
  5. Replace the Selector (**Sel:**) field with “1d”.
  6. Click **Add** and then **Save**. The TID has been added to the pull-down menu for this CIT. If you replace the SYSCTL in the GNE, re-enter the NSAP address for this GNE's TID.

11 Select the **FTP** tab.

12 Select the connection from the **Profile** pull-down menu and then proceed to Step 14. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the download to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user name/password can be different.)

13 If you entered connection information in Step 12 and wish to keep the information for future backups:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

Important! Entries to the **Profile** pull-down menu can be changed using the **Modify**, **Apply**, and **Save** buttons or removed using the **Delete** button.

14 In the **Source/Destination Directory Path** panel, enter the current location of the generic to be downloaded or use the **Browse** button (if available) to select the generic to be downloaded. If the FTP server is either undefined or not the local host, the **Browse** button is greyed out.

Important! If you selected the default installation location for the *WaveStar*® CIT and software generic: **`\generics\DMX\9.1.x\p`**. If necessary, replace 9.1.0 with your current release, for example 9.1.1. The *WaveStar*® CIT automatically populates the FTAM Responder and NSAP fields. Click **Next**.

The value of the Path field can be either an absolute path or a relative path that is relative to the FTAM server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: **`C:\Program Files\Alcatel-Lucent\WaveStar CIT\generics\DMX\9.1.x\p`**. If necessary, replace 9.1.0 with your current release, for example 9.1.1. The syntax of the relative path must start with the path name; for example: **`\generics\DMX\9.1.x\p`**.

15 In the **Product Type** panel, select the product type of the software generic that you are downloading (not necessarily the same as the NE to which you are downloading).

16 Click **OK**.

Result: A warning message appears asking you to confirm executing this command. Verify the information and click **Yes**. While the download is in progress, a progress indicator window is present.

The download takes approximately 30 minutes.

The download can be cancelled any time by pressing the **Cancel** button on the progress screen.

When the transfer is complete, the *Progress Indicator* window closes and the download software successful window appears. Click **OK**.

17 Do you wish to observe the FTP download progress?

If...	Then...
Yes	Proceed to Procedure 6-24: "Observe FTP progress" (p. 6-285) and then continue with Step 18.
No	Continue with Step 18.

18 **Important!** Do NOT insert a new circuit pack in the shelf until after you apply the new software generic and clear the `dormant/exec version mismatch` condition.

Do you wish to apply (activate) the software generic that you recently downloaded to the dormant area of the Alcatel-Lucent 1665 DMX shelf?

If...	Then...
Yes	Proceed to Procedure 6-20: "Apply software generic" (p. 6-249) and then continue with Step 19.
No	Continue with Step 19.

19 Do you wish to upgrade additional shelves via FTTD?

If...	Then...
Yes	Repeat this procedure from Step 2 for each shelf that you wish to upgrade via FTTD.
No	STOP! End of Procedure.

END OF STEPS

Procedure 6-19: Upgrade software generic via FTAM

Overview

Use this procedure to upgrade the software generic to Release 9.1.x via the File Transfer and Access Management (FTAM) protocol.

Note: You can upgrade directly to 9.1.x from the following releases:

- R5.1.3/5.1.7
- R7.1.2
- R8.0.2/R8.0.3/8.0.4/8.0.5/8.0.6
- R9.0.1

You must complete a two-step upgrade to 9.1.x from the following releases:

- R6.0.1/6.0.2/6.0.4 through R8.0.5
- R7.0.2 through R8.0.5
- R7.1.1/7.1.4 through R8.0.6

You must complete a three-step upgrade to 9.1.x from R5.1.4/5.1.5 through R7.0.2, and then through R8.0.5.

To download the software generic to a local shelf using SFTP, refer to Procedure 6-16: “Ugrade software generic via SFTP” (p. 6-171).

To download the software generic to a local shelf via FTP, refer to Procedure 6-17: “Upgrade software generic via FTP” (p. 6-175).

To download the software generic to a remote shelf via FTTD, refer to Procedure 6-18: “Upgrade software generic via FTTD” (p. 6-212).

Important! You must have OSI connectivity (via your OSI LAN or DCC) to the network element to use FTAM.

Privilege level

You must log in as a Privileged user to complete this procedure.

Required equipment

In addition to “Required equipment” (p. 6-3) listed in this chapter, the following equipment is also required:

- CAT5 Ethernet cable with either a 10/100 hub or a cross-over cable for the **LAN** or **IAO LAN** port (required for TCP/IP connectivity)
- Copy of the new system generic software program accessible from your PC. Refer to Procedure 6-1: “Install software on the PC” (p. 6-4).

- Factory-fresh LNW2, system controller (SYSCTL), with two factory-installed non-volatile memory (NVM) cards installed
- Current *Alcatel-Lucent 1665 Data Multiplexer (DMX) Software Release Description* for the software generic being installed

Before you begin

Before performing this procedure:

1. Refer to "Before you begin" (p. 6-3) and "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".
2. Verify that new software generic program is available.
3. Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Software Release Description* for a description of any special considerations required when installing this version of software.
4. The SYSCTL must have Alcatel-Lucent 1665 DMX 5.1.3 or later software generic to upgrade the software generic program to 9.1.x via FTAM.

Steps

Complete the following steps to upgrade the software generic via the FTAM protocol.

1 Connect the cross-over LAN cable from the Network Interface Card (NIC) on the PC to the front **LAN** port on the SYSCTL circuit pack faceplate and establish a *WaveStar*® CIT session. (When TCP/IP is enabled on the rear LAN port **J16 IAO LAN**, OSI is disabled.)

Double-click the *WaveStar*® CIT icon on your desktop and login (if necessary), to start the *WaveStar*® CIT software on the PC. Refer to Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27).

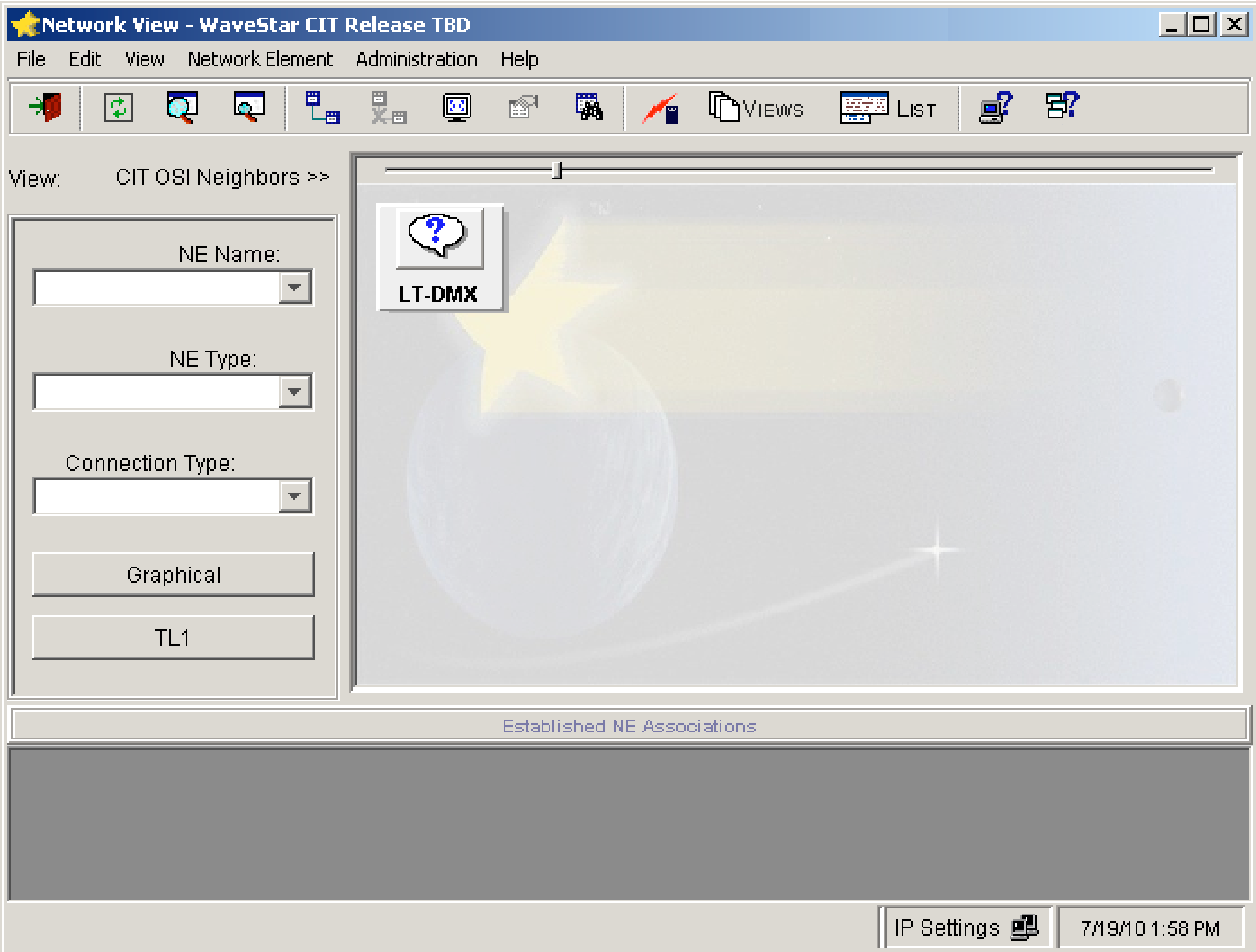
Result: The *Network View* appears.

2 From the **View:** pull-down menu, select **CIT OSI Neighbors**.

Important! This **View:** is not the menu bar item View → ...; it is located above the NE Name pull-down menu.

Result: The CIT OSI neighbor(s) are automatically detected.

If you were previously logged in to the NE and/or you do not see your NE, from the Network View, select **View** → **Refresh OSI View**.



3 In the Network View, right-click the NE icon that was detected (default TID is LT-DMX, your TID can be different), and select **Graphical Using** → **OSI** from the resulting menu.

Result: The *System Type Selection* window appears.

4 In the *System Type Selection* window, select DMX and click **OK**.

Result: The *NE Login Dialog* window appears.

5 In the NE login window, login to the shelf using your user ID and password. Click **OK**.

6 From the System View menu, select **View** → **Equipment**, highlight the SYSCTL, and click **Select**.

Result: The *View Equipment* window appears. Record the Apparatus Code and the Program Version.

7 What is the apparatus code of your SYSCTL and what program version (software generic Release x.x.x) is it currently running?

If...	Then...
Apparatus Code = LNW1 Program Version = 3.1, 4.0, 5.0	You must upgrade your software to Release 5.1.3 and then repeat this procedure from Step 1.
Apparatus Code = LNW1 Program Version = 5.1.3/5.1.7	Proceed to Procedure 6-19.1: "Verify proper equipage in Main slots" (p. 6-222).
Apparatus Code = LNW1 Program Version = 5.1.4/5.1.5	You must upgrade your software to Release 7.0.2 and then repeat this procedure from Step 1.
Apparatus Code = LNW2 Program Version = 6.0.x (x=1, 2, 4) or 7.0.2	You must upgrade your software to Release 8.0.6 and then repeat this procedure from Step 1.
Apparatus Code = LNW2 Program Version • 7.1.x (x=1, 2, 4) • 8.0.x (x=2, 4, 5, 6) • 9.0.1	Proceed to Procedure 6-19.3: "Upgrade software generic via FTAM (7.1.x, 8.0.x, 9.0.1 or later to 9.1.x)" (p. 6-246).

END OF STEPS

Procedure 6-19.1: Verify proper equipage in Main slots

Overview

Use this procedure to verify that the Main slots are equipped with circuit packs that are supported in 9.1.x.

LNW26 circuit packs are not supported in 9.1.x.

Since LNW26B-type circuit packs with the jumper set to *NORMAL* are identical to LNW26 circuit packs, LNW26B-type circuit packs (LNW26B, LNW28, LNW77, LNW121B-151B) with the circuit pack mode jumper set to *NORMAL* (six STS-1 switch fabric) are not supported in 9.1.x. The jumper on LNW26B-type circuit packs must be set to *ENHANCED* (12 STS-1 switch fabric) to use these circuit packs in 9.1.x.

> **Important!** If you determine that the Main slots in your NE are equipped with unsupported circuit packs, you must upgrade those circuit packs before upgrading to 9.1.x.

Required equipment

Refer to "Required equipment" (p. 6-218) in Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure:

1. Complete Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218).
2. If your Main slots contain unsupported circuit packs, you must have access to supported circuit packs.

Steps

Complete the following steps to verify that supported equipment is installed in your shelf.

1 From the System View menu, select **Reports** → **Equipment Lists** → **Pack**, highlight **Shelf**, and click **Select**.

Result: The *Circuit Pack List* screen appears.

2 In the *Circuit Pack List* screen, locate the *main-1-cp* and *main-2-cp* AIDs in the Circuit Pack AID column. Are the Apparatus Codes for those AIDs either LNW26 or LNW26B-type (LNW26B, LNW28, LNW77, LNW121B-151B)?

If...	Then...
Yes (LNW26)	You must upgrade the LNW26 circuit packs in the Main slots to supported circuit packs. Refer to *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* for detailed instructions about upgrading circuit packs and then repeat this procedure.
Yes (LNW26B, LNW28, LNW77, LNW121B-151B)	Continue with Step 3 to determine the circuit pack mode of the packs.
No	The Main slots are equipped with circuit packs that are compatible with 9.1.x. Proceed to Procedure 6-19.2: "Upgrade software generic via FTAM (5.1.3/5.1.7 to 9.1.x)" (p. 6-225).

3 From the System View menu, select **View** → **Equipment** → **Circuit Pack**, highlight CP main-1, and click **Select**.

Result: The *View Equipment* screen appears.

4 In the *View Equipment* screen, locate the Circuit Pack Mode parameter in the Equipment Details panel. Note the value of the Circuit Pack Mode for CP Main-1, either *NORMAL, or ENHANCED*.

Do NOT click **Close** on the *View Equipment* screen.

5 Highlight CP main-2 and click **Select**.

6 In the *View Equipment* screen, locate the Circuit Pack Mode parameter in the Equipment Details panel. Note the value of the Circuit Pack Mode for CP Main-2, either *NORMAL, or ENHANCED*.

7 Refer to Step 4 and Step 6. Is the Circuit Pack Mode for CP main-1 and/or CP main-2 *NORMAL* (six STS-1 switch fabric)?

If...	Then...
Yes	The LNW26B-type circuit packs with the Circuit Pack Mode jumper set as *NORMAL* are NOT supported in 9.1.x. Choose one of the following two options: 1. Change Circuit Pack Mode to *ENHANCED* by physically changing the jumper setting on the circuit packs. Proceed to Procedure 6-5: "Replace high-speed main OLIU circuit pack" (p. 6-48) for detailed instructions on changing jumper settings and then repeat this procedure. 2. Upgrade the LNW26B-type circuit packs to LNW27, LNW29, LNW32, LNW76, LNW202, or LNW221–259 OC-48 OLIU circuit packs. These circuit packs can cross-connect VT1.5 signals in up to 48 STS-1 signals. Refer to *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* for detailed instructions about upgrading circuit packs and then repeat this procedure.
No	The LNW26B-type circuit packs with the Circuit Pack Mode jumper set as *ENHANCED* are supported in 9.1.x. Proceed to Procedure 6-19.2: "Upgrade software generic via FTAM (5.1.3/5.1.7 to 9.1.x)" (p. 6-225) to upgrade the 5.1.x shelf to 9.1.x.

END OF STEPS

Procedure 6-19.2: Upgrade software generic via FTAM (5.1.3/5.1.7 to 9.1.x)

Overview

Use this procedure to upgrade a software generic from Release 5.1.3/5.1.7 to Release 9.1.x via FTAM.

Required equipment

Refer to "Required equipment" (p. 6-218) in Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure:

1. Complete Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218).
2. You must be able to perform a backup of the R5.1.x database.

Steps

Complete the following steps to upgrade a software generic from Release5.1.3/5.1.7 or later to Release 9.1.x.

1 From the System View menu, select **Configuration** → **Software** → **Remote Backup**.

2 In the pull-down **Backup To/Via:** menu, select **FTAM**.

3 In the **Source/Destination Directory Path** field, enter **`\backups\<filename>`**.

You can also click the **Browse** button next to the *Path:* field to browse to any directory on your PC.

> **Important!** The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.
>
> The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is
>
> `C:\Program Files\Alcatel-Lucent\WaveStar CIT\`

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.

If you wish to store your data in a subdirectory, enter **`\backups\<subdirectory>\<filename>`** if the subdirectory exists before the command is sent. If any directory in the path does not exist, the command is denied because this command does not create directories.

4 Click **OK**.

You are asked to verify that you wish to backup to the directory that you entered. Click **Yes** if you typed the path correctly.

Result: The *Progress Indicator* screen appears, indicating that the backup is in progress. When the backup completes, a `Remote Backup successful` screen appears. Click **OK**. The backup file is now stored. If the default path and a subdirectory were used, the file can be found at:

```
C:\Program Files\Alcatel-Lucent\\WaveStar CIT\backups\
<subdirectory>\<filename>
```

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\.

5 Close your *WaveStar*® CIT session with the 5.1.x NE. From the System View, select **File** → **NE Disconnect** and click **Yes** in the confirmation window.

Result: The *System View* closes.

6 Disconnect the LAN and/or serial cables from the **LAN** and/or **RS232** port(s) on the front of the LNW1 SYSCTL.

7 Initiate a ten-second countdown (9, 8, 7, 6, 5, 4, 3, 2, 1, 0) in the **IND** display on the LNW1 SYSCTL by simultaneously depressing the **ACO TEST** and **SEL** buttons on the front of the LNW1 SYSCTL.

Important! Removing the LNW1 without initiating the ten-second countdown can result in unexpected and undesirable protection switches, incorrect circuit fault indications, or incoming signal failure alarms. All SYSCTL functions are suspended during the countdown.

8 Remove the LNW1 SYSCTL circuit pack during the 10-second countdown.

Important! While the SYSCTL circuit pack is removed, do *NOT* remove or replace any transmission circuit packs.

9 **Important!** For software installation, ensure that two NVMs are present in the LNW2 SYSCTL. After the LNW2 is installed, if one or two NVMs are missing, `NVM removed` alarm(s) are issued. If both NVM sockets are empty, the **IND** displays an alternating **E** and **0** and **1**.

Refer to Step 10 for the complete listing of codes and required actions.

Seat the new LNW2 SYSCTL circuit pack and allow a few minutes for the pack to complete initialization.

Result: The LNW2 SYSCTL exhibits the following visible cycles during initialization:

1. The **FAULT** LED lights and remains lighted for approximately 90 seconds. After approximately 10 seconds, a flashing **b** appears in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 75 seconds and the **IND** display is blank.
2. The **FAULT** LED remains lighted for approximately another 20 seconds and then extinguishes.
3. The **ACTIVE** LED lights and remains lighted and the **CR** LED flashes 10 times. While the **CR** LED is flashing, the **MJ**, **ABN**, and **NE** LEDs light and remain lighted.
4. Continue with Step 10.

10 Observe the **IND** display on the LNW2 SYSCTL; the display indicates the state of the SYSCTL.

If...	Then...
alternating **M** and **P** and **6** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	6.0 Maintenance Mode. Continue with Step 11.
alternating **M** and **P** and **7** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	7.0 Maintenance Mode. Continue with Step 11.
alternating **M** and **P** and **7** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **1**	7.1 Maintenance Mode. Continue with Step 11.

If...	Then...
alternating **M** and **P** and **8** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	8.0 Maintenance Mode. Continue with Step 11.
alternating **M** and **P** and **9** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **0**	9.0 Maintenance Mode. Continue with Step 11.
alternating **M** and **P** and **9** and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **1**	9.1 Maintenance Mode. Continue with Step 11.
alternating **E** and **0** and **0**	LNW2 SYSCTL must be replaced. Find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
alternating **E** and **0** and **1**	No NVMs are detected on the LNW2 SYSCTL. Install two Alcatel-Lucent-supplied NVMs in the LNW2 or find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
alternating **E** and **0** and **2**	NVMs are present but not readable. Check to make sure they are properly seated and repeat this procedure.
alternating **E** and **0** and **3**	Not Supported. Find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
alternating **E** and **1** and **0**	LNW2 SYSCTL does not boot. No compatible generic on the NVMs in the LNW2 SYSCTL. Find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure or contact your next level of support.
Letter **F**	LNW2 SYSCTL faceplate latches are not fully seated. Unseat the LNW2 SYSCTL and repeat this procedure, properly seating the faceplate latch.

If...	**Then...**
alternating **N** and **O** and **x**	"x" indicates that the NVM socket (1 or 2) is empty or the NVM installed is failed. Replace the indicated NVM or find another LNW2 SYSCTL equipped with two factory-installed NVMs and repeat this procedure.
Letter **U**	LNW2 SYSCTL does not boot due to unexpected or unreadable shelf type. Repair the problem generally caused by bent pins and repeat this procedure.
flashing **b**	Boot in progress.
A red, four-segment square (2 x 2) appears in the **IND** display on the LNW2 SYSCTL.	Acknowledges the **UPD/INIT** button was momentarily pushed. Pushing the **UPD/INIT** button while in Maintenance Mode has no effect.

11 Connect the cross-over LAN cable from the Network Interface Card (NIC) on the PC to the front **LAN** port on the SYSCTL circuit pack faceplate and establish a *WaveStar*® CIT session. (When TCP/IP is enabled on the rear LAN port **J16 IAO LAN**, OSI is disabled.)

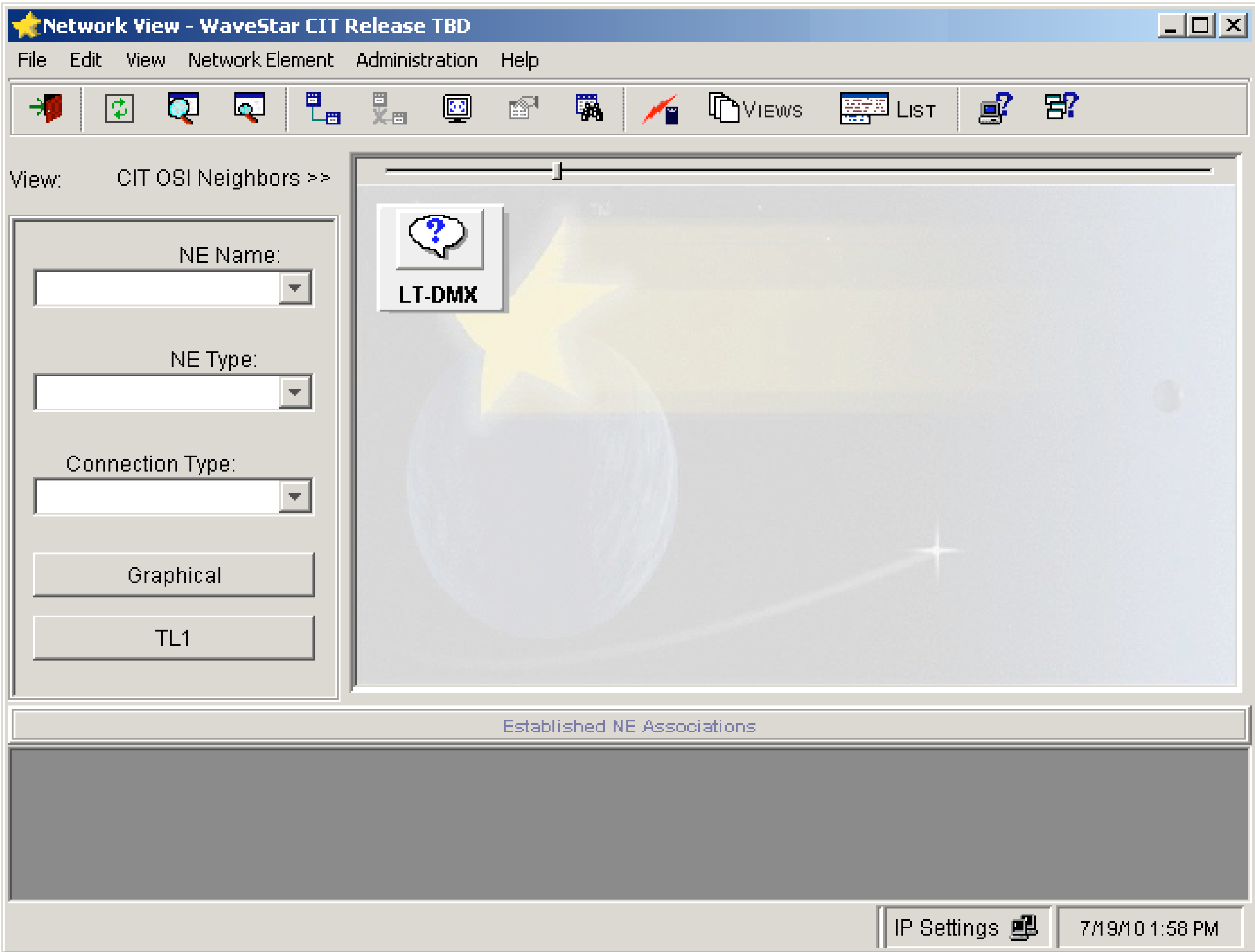
12 From the Network View of the *WaveStar*® CIT session you established in Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218), select the **View:** pull-down menu and select **CIT OSI Neighbors**.

Important! This **View:** is not the menu bar item View → ...; it is located above the NE Name pull-down menu.

13 From the Network View, select **View** → **Refresh OSI View**.

Result: The CIT OSI neighbor(s) are automatically detected.

Your TID is LT-DMX; when in Maintenance Mode, the TID is always default.



14 In the Network View, right-click the LT-DMX NE icon that was detected, and select **Graphical Using** → **OSI** from the resulting menu.

Result: The *System Type Selection* window appears.

15 In the *System Type Selection* window, select DMX and click **OK**.

Result: The *NE Login Dialog* window appears.

16 **Important!** Because the shelf is in Maintenance Mode, your logins and passwords are default.

Enter the following in the *NE Login Dialog* window (login information is case sensitive) to log in to the NE:

User ID: ***LUC01***

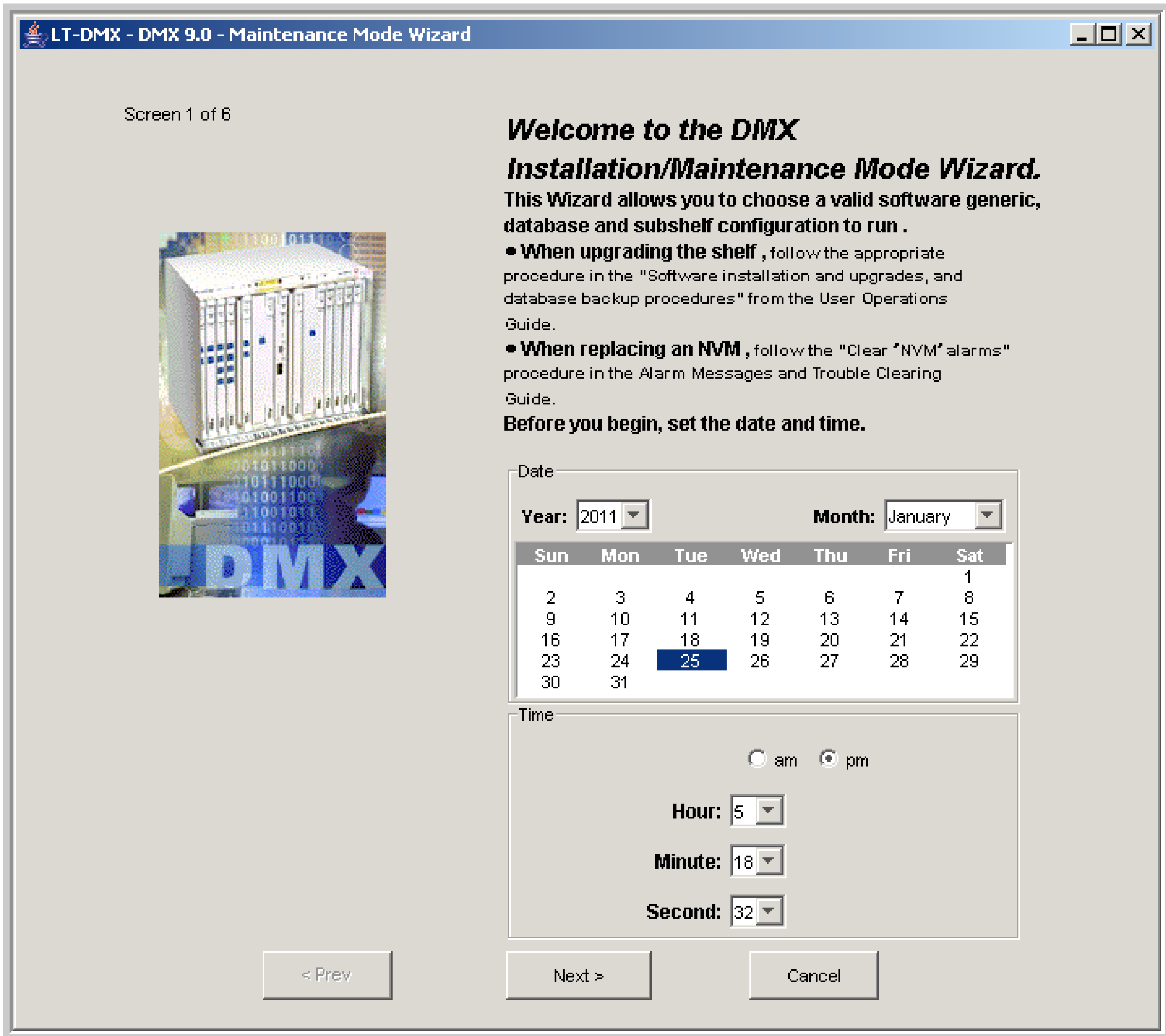
Password: ***DMX2.5G10G***

Click **OK**.

Important! After you select your backup database, complete the Maintenance Mode Wizard, and the NE restarts, your original User IDs and Passwords are restored.

Result: Screen 1 of 6 in the Maintenance Mode Wizard appears.

Depending on the boot code of your SYSCTL (refer to Step 10), the title bar of the Maintenance Mode Wizard displays either DMX 6.0, DMX 7.0, DMX 7.1, DMX 8.0, DMX 9.0, or DMX 9.1



This screen picks up the time format preference from the *WaveStar*® CIT.

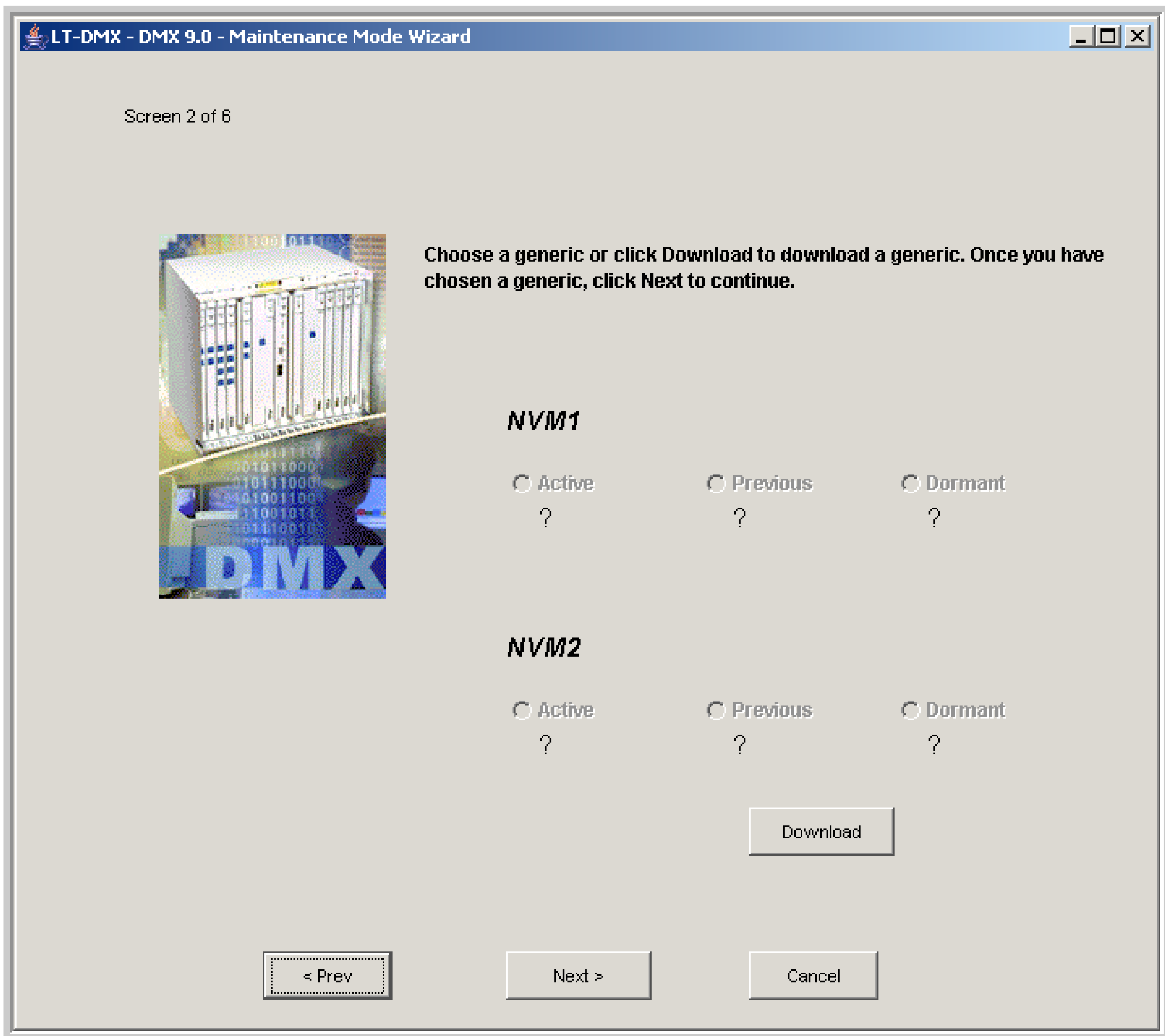
You can provision the time format display for your *WaveStar*® CIT from the Network View by selecting **View** → **Preferences** and clicking the Display tab. This screen allows you to choose your preference for time format, either a 12-hour clock or a 24-hour clock.

- If your time format preference is a 12-hour clock, from the **Time** panel, select **Hour:** (0–12), **Minute:** (0–59), and **Second:** (0–59) from the pull-down menus. You must also specify am or pm by selecting one of the radio buttons.
- If your time format preference is a 24-hour clock, From the **Time** panel, select the **Hour:** (0–23), **Minute:** (0–59), and **Second:** (0–59) from the pull-down menus.

17 **Important!** The actual time and date are preset from your PC.

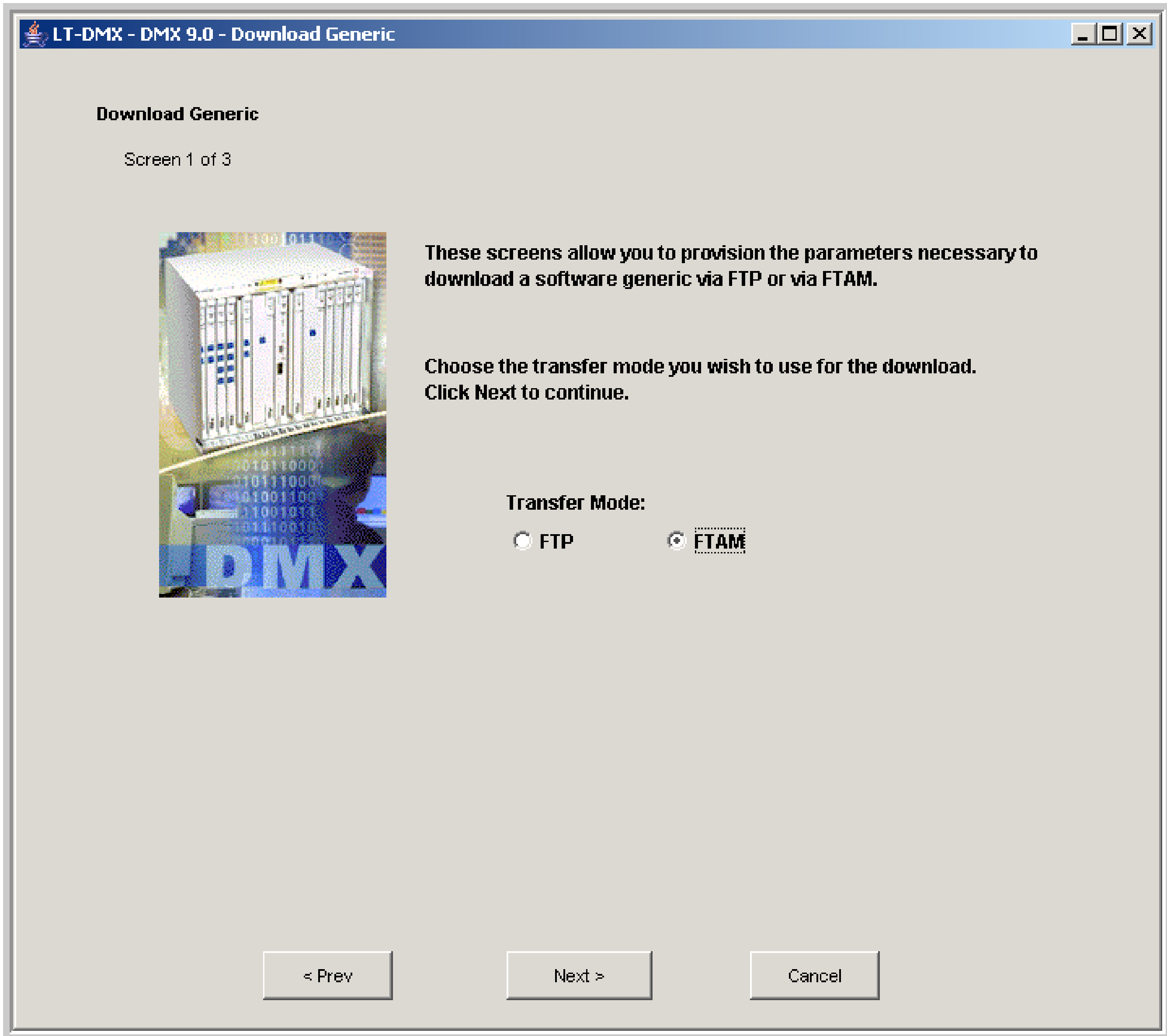
On Screen 1 of 6 in the Maintenance Mode Wizard, read the information, verify the date and time, make any required changes, and click **Next**.

Result: Screen 2 of 6 in the Maintenance Mode Wizard appears.



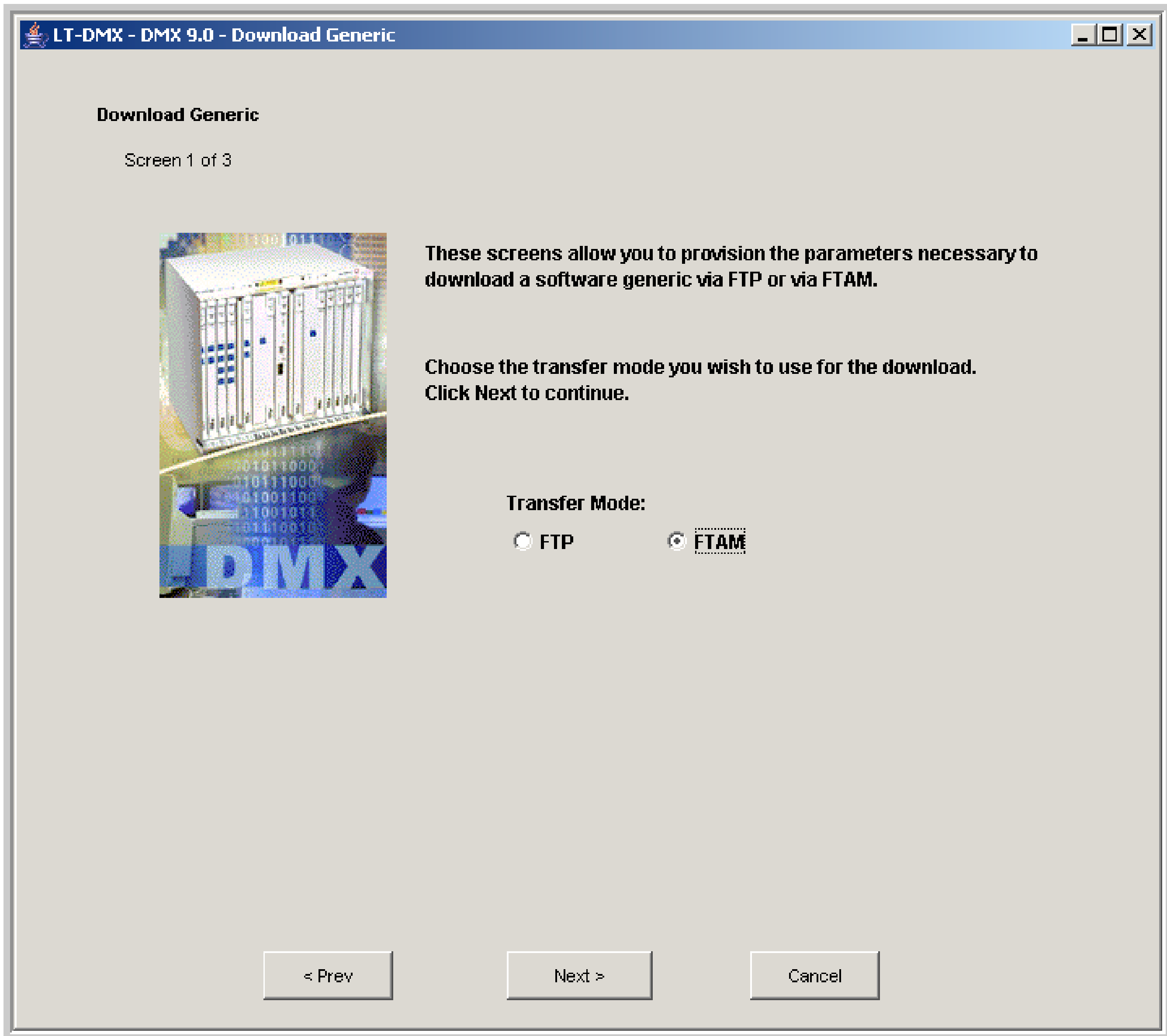
18 On Screen 2 of 6 in the Maintenance Mode Wizard, click **Download**.

Result: Screen 1 of 3 in the Download Generic Wizard appears.



19 On Screen 1 of 3 in the Download Generic Wizard, read the information, select **FTAM** and click **Next**.

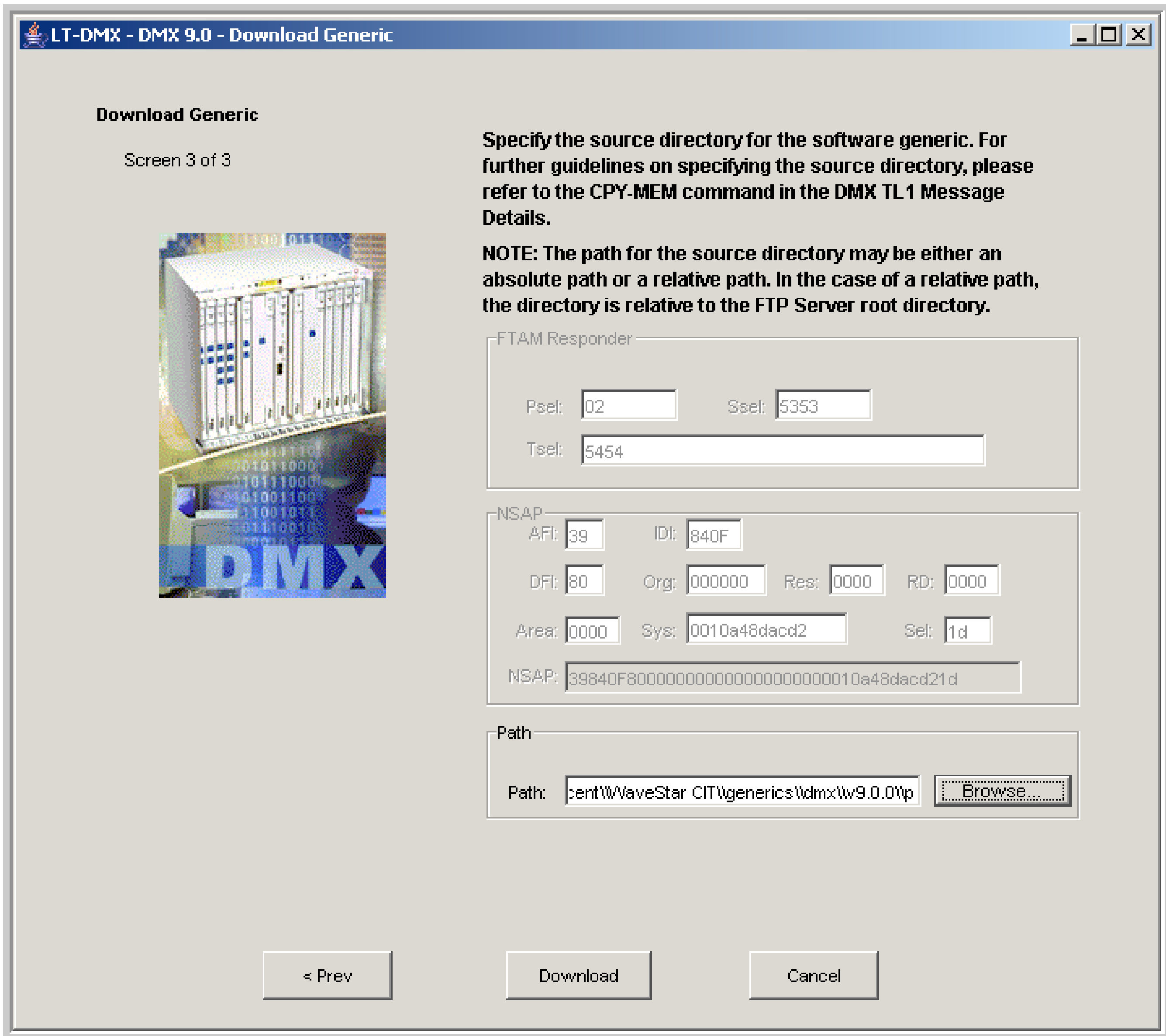
Result: Screen 2 of 3 in the Download Generic Wizard appears.



20 **Important!** LAN-1 is the **LAN** port on the faceplate of the LNW2 SYSCTL circuit pack. LAN-2 is the **J16 IAO LAN** port on the rear of the Alcatel-Lucent 1665 DMX shelf.

On Screen 2 of 3 in the Download Generic Wizard, read the information, verify that the LAN port you are connected to has OSI Function Enable selected, and click **Next**.

Result: Screen 3 of 3 in the Download Generic Wizard appears.



21 On Screen 3 of 3 in the Download Generic Wizard in the **Path** panel, enter the current location of the generic to be downloaded in the Path field or use the **Browse** button to select the generic to be downloaded. Click **Download**.

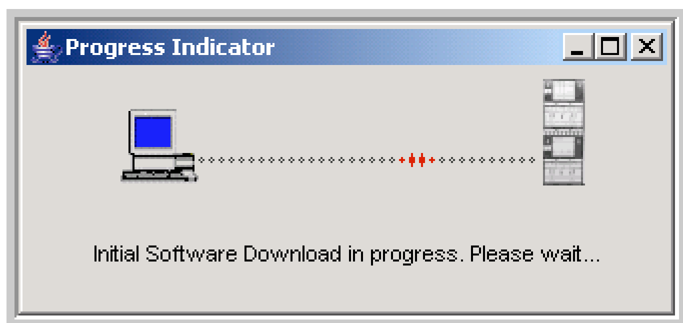
The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: **`C:\Program Files\Alcatel-Lucent\WaveStar CIT\generics\DMX\9.1.x\p`**. The syntax of the relative path must start with the path name; for example: **`\generics\DMX\9.1.x\p`**. If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, your path could start with C:\Program Files\Lucent Technologies\. If necessary, replace 9.1.0 with your current release, for example 9.1.1.

Result: A warning message appears listing the options you provisioned in the previous screens.

---

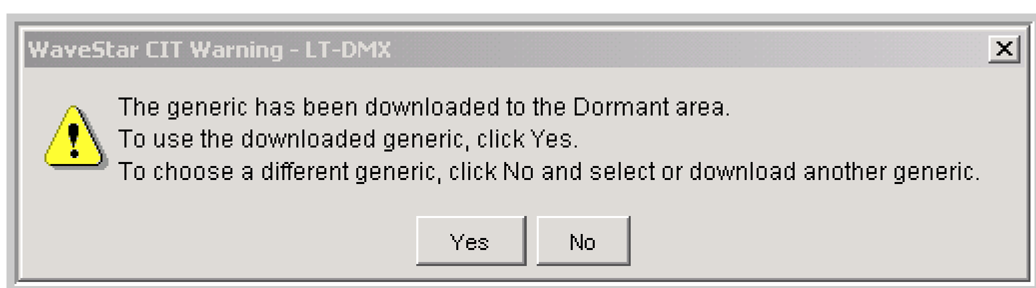
22 Verify the information and either click **Yes** to start the download process or click **No** to return to the download screen and change your selections.

Result: If you choose yes, the following initial software download progress indicator runs for approximately 30 minutes.

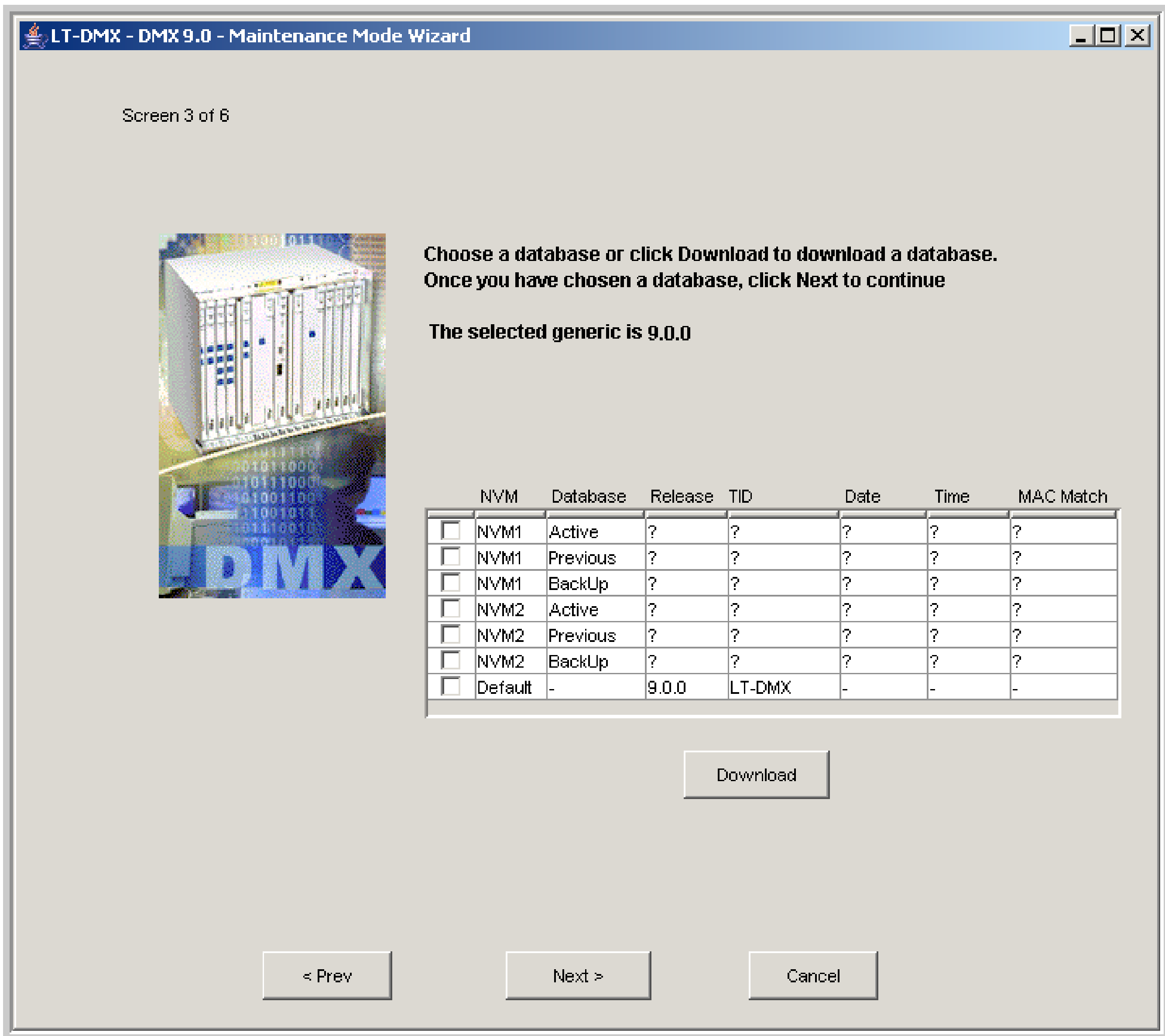


---

23 Once the software generic download is complete, the following confirmation message appears. Click **Yes** to use the generic that is now in the Dormant area.



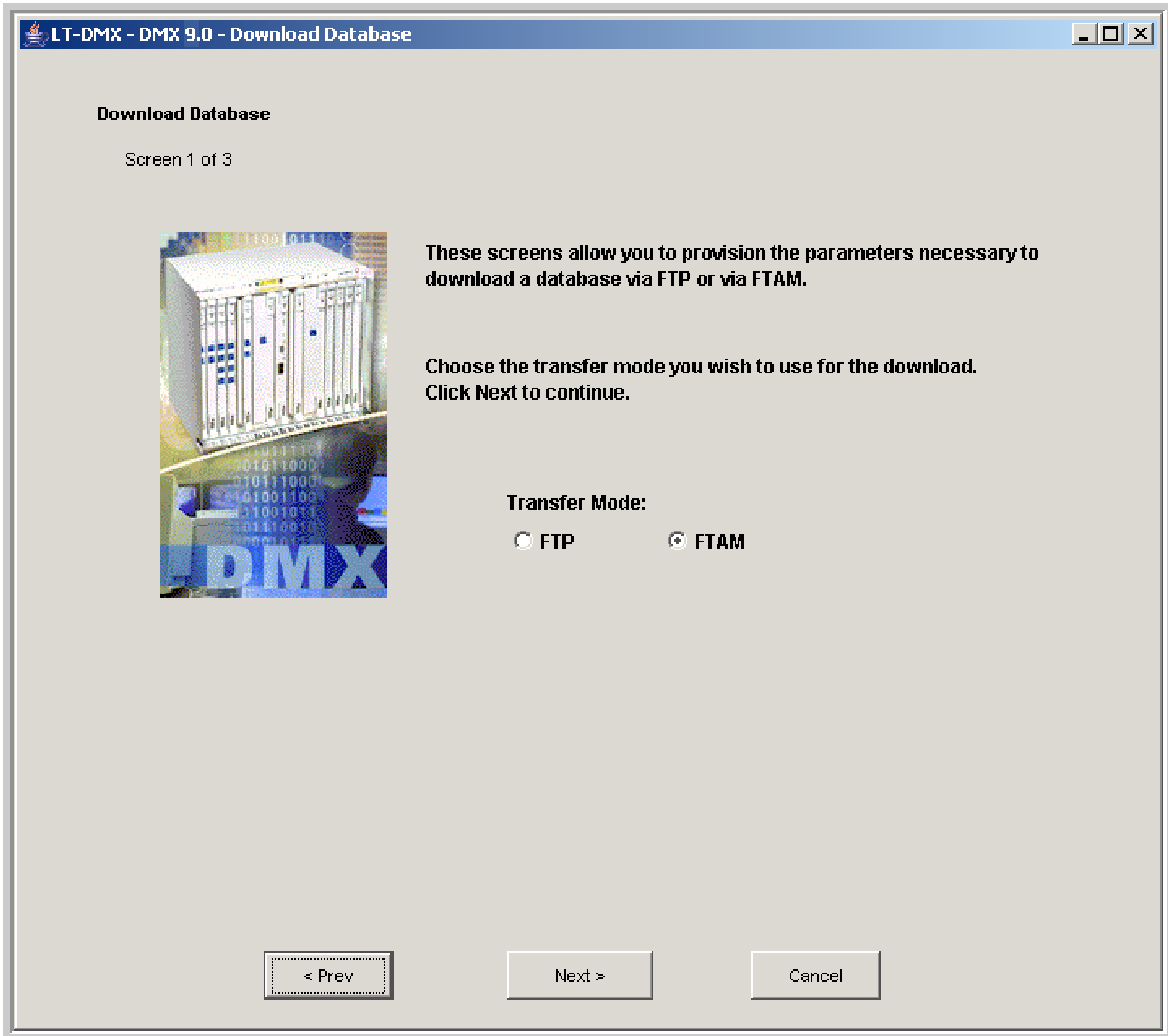
Result: Screen 3 of 6 in the Maintenance Mode Wizard appears.



24 **Important!** Do NOT select the default database or you could loose service to your shelf. You MUST download your previously backed up database.

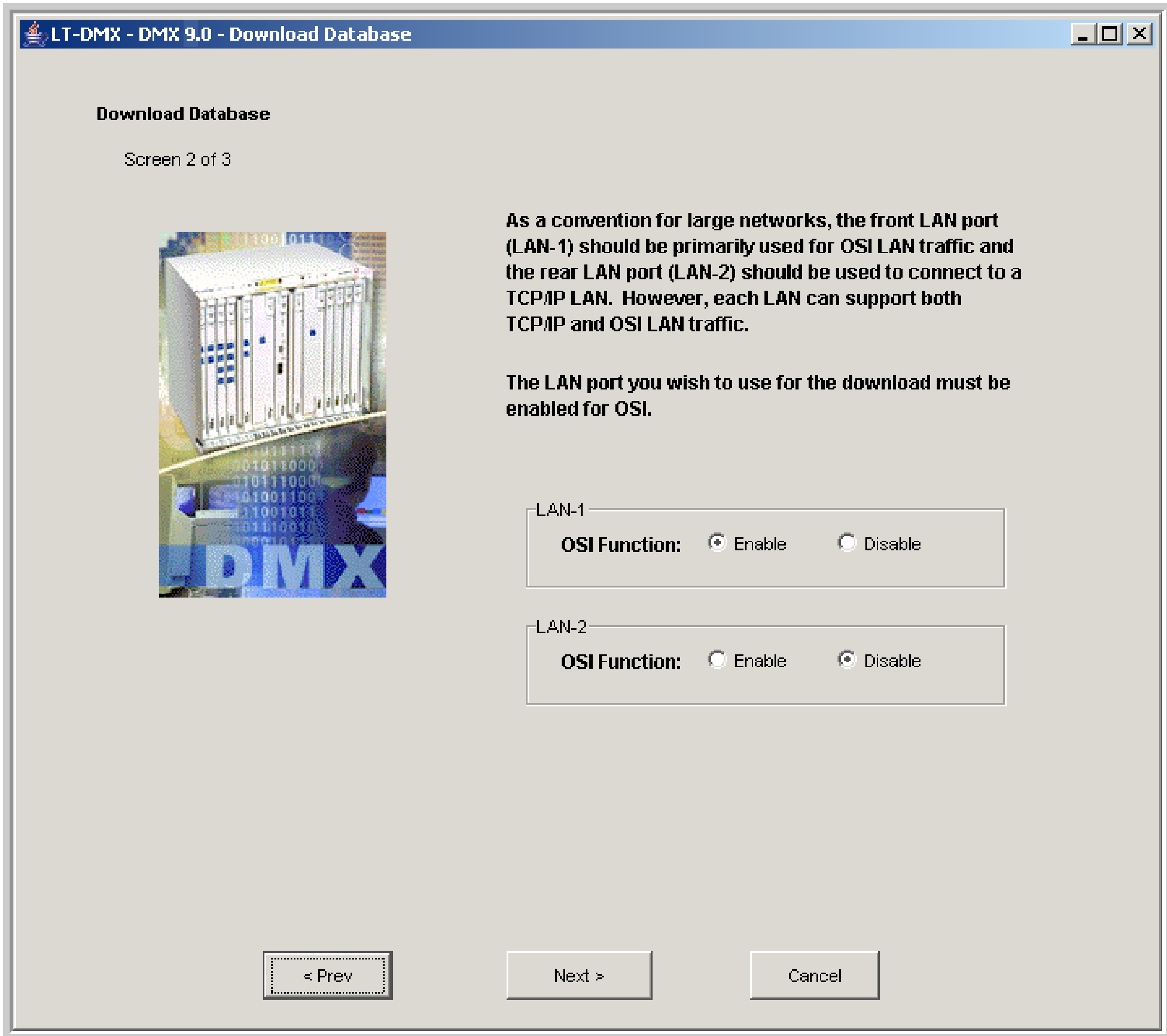
On Screen 3 of 6 in the Maintenance Mode Wizard, click **Download**.

Result: Screen 1 of 3 in the Download Database Wizard appears.



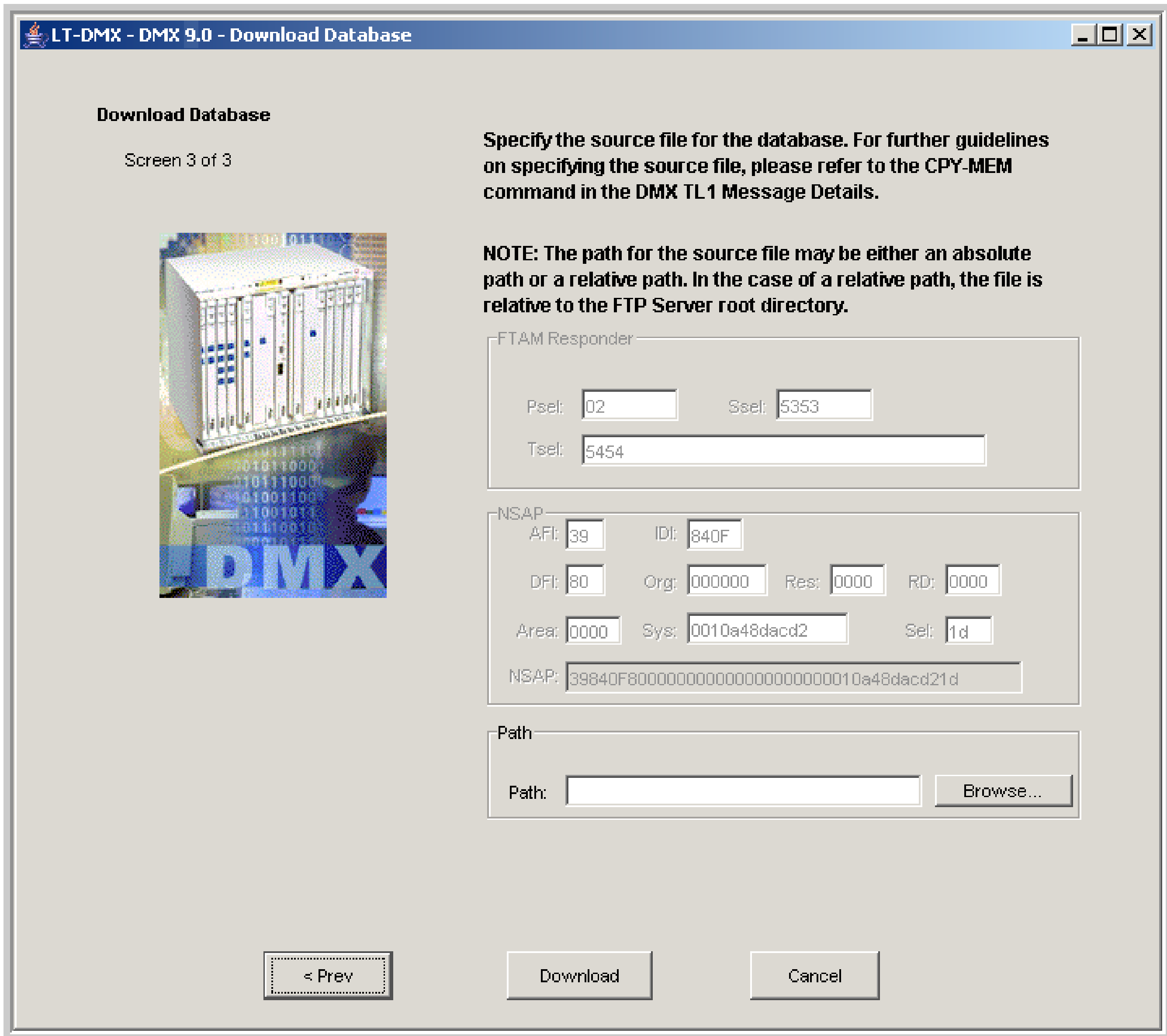
25 On Screen 1 of 3 in the Download Database Wizard, read the information, select **FTAM** and click **Next**.

Result: Screen 2 of 3 in the Download Database Wizard appears.



26 On Screen 2 of 3 in the Download Database Wizard, read the information, verify that the LAN port you are connected to has OSI Function Enable selected, and click **Next**.

Result: Screen 3 of 3 in the Download Database Wizard appears.



27 On Screen 3 of 3 in the Download Database Wizard in the **Path** panel, enter the location where the database information is stored. Enter the path and filename exactly as it was entered in Step 3. For example: **`\backups\<subdirectory>\<filename>`**.

You can also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and select the required file.

Click **Download**.

Important! The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.

The *WaveStar®* CIT directory automatically enters the relative path for the *WaveStar®* CIT. The default relative path is

`C:\Program Files\Alcatel-Lucent\WaveStar CIT\`

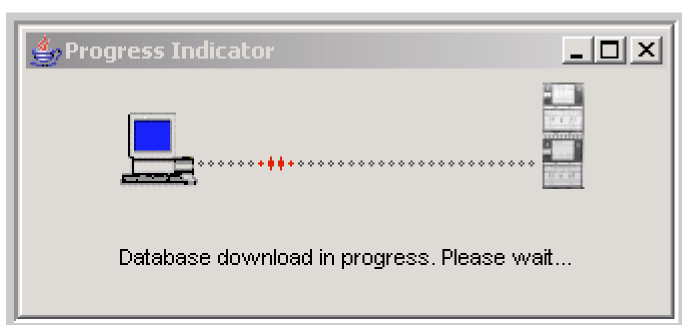
If you had an older *WaveStar®* CIT installed prior to installing the current *WaveStar®* CIT, your path could start with C:\Program Files\Lucent Technologies\.

Result: A warning message appears listing the options you provisioned in the previous screens.

---

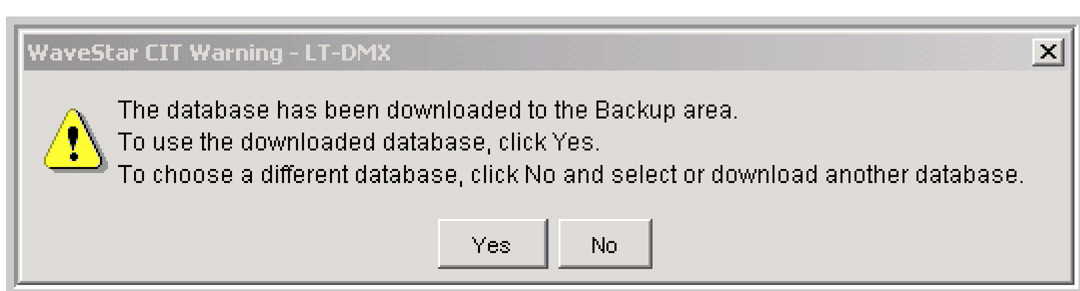
28 Verify the information and click **Yes**.

Result: If you choose Yes, the database download progress indicator runs for approximately two minutes.

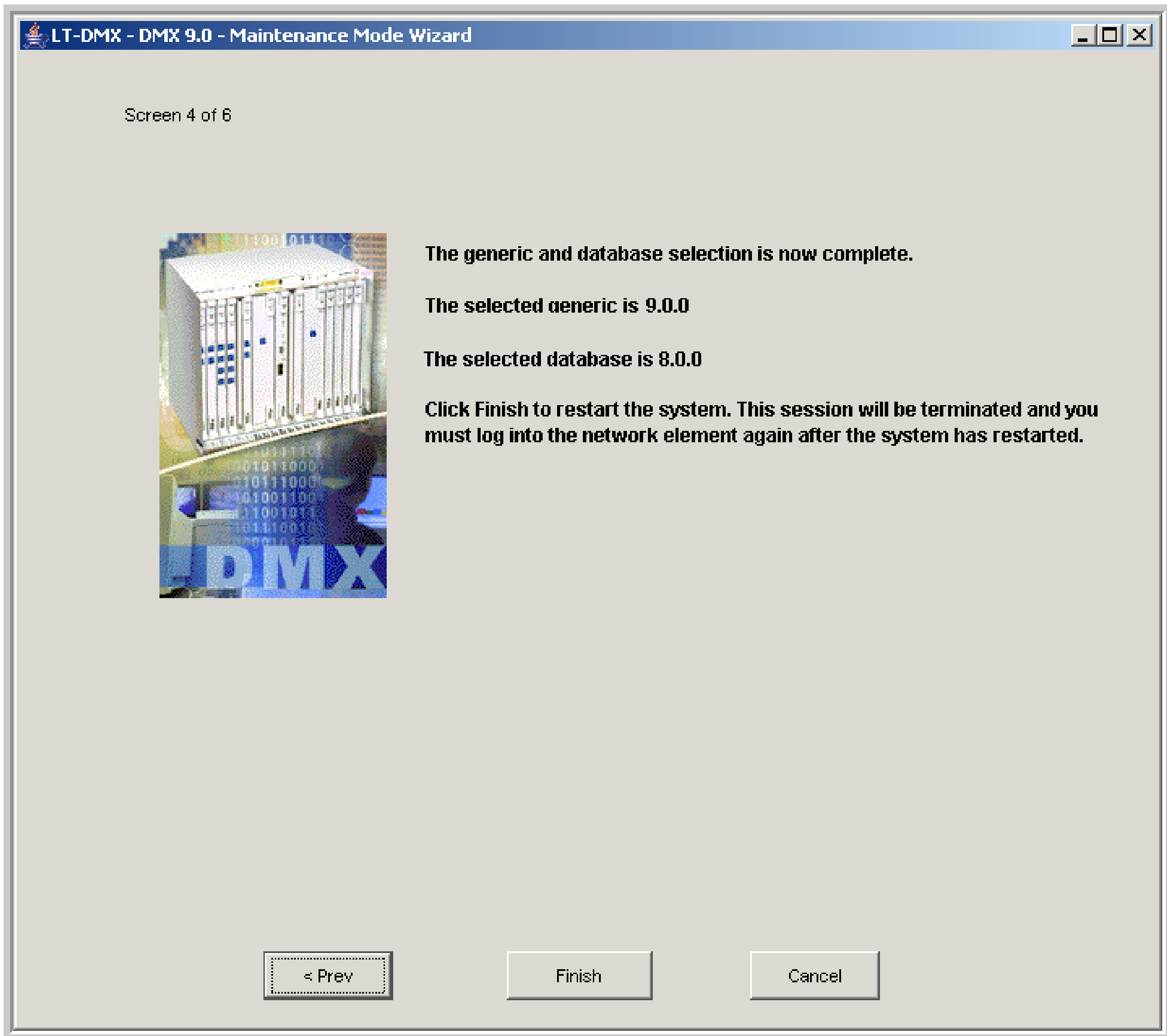


---

29 Once the database download is complete, the following confirmation message appears. Click **Yes** to use the database that is now in the Backup area.



Result: Screen 6 of 6 in the Maintenance Mode Wizard appears. In this screen, 9.1.0 is an example; your selected generic could be different, for example 9.1.1. 5.1.3 is an example too; your selected database could be 5.1.7



30 On Screen 6 of 6 in the Maintenance Mode Wizard, read the information, verify that you have selected the correct generic and database, and click **Finish** to restart the system and apply the generic and database.

Result: The Maintenance Mode Wizard closes and your connection to the shelf is terminated.

The LNW2 SYSCTL exhibits the following visible cycles while the generic and database are installed and validated and the SYSCTL reboots:

1. For approximately 12 minutes, the alternating **M** and **P** and **X** (X represents 6, 7, 8, or 9, depending on your Maintenance Mode) and "**.**" ("." is a red, four-segment square [2 x 2] representing a period) and **Y** (Y represents 0 or 1, depending on your Maintenance Mode) continue to appear in the **IND** display on the SYSCTL.
2. After approximately 12 minutes, all LEDs extinguish and the **IND** display on the SYSCTL is blank for approximately 5 seconds.
3. A flashing **b** appears in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 60 seconds and the **IND** display is blank for approximately 20 seconds.
4. The **ACTIVE** LED lights and remains lighted.
5. A flashing **b** appears again in the **IND** display on the SYSCTL, indicating that a boot is in progress. The **b** continues flashing for approximately 2.5 minutes while the database is being converted and the **IND** display is blank.
6. When nothing appears in the **IND** display and the **ACTIVE** LED is lighted and the other LEDs return to their previous state (pre-LNW1 backup), the NE software and database installation is complete.

   However, smart circuit packs can be upgrading their firmware. If flashing green **ACTIVE** LEDs are present on a circuit pack, firmware is currently being downloaded to that pack. Wait until all smart circuit packs finish upgrading their firmware before proceeding.

   If an alarm condition existed before the upgrade, the NE rediscovers the alarm condition and activate the appropriate LEDs on the shelf.
7. Continue with Step 31.

---

31 To verify that the upgrade was successful, depress and hold the **ACO TEST** push-button on the LNW2 SYSCTL for about 4 seconds.

Result: All LEDs on the shelf light. A red, 35-segment (5 x 7) rectangle appears in the **IND** display on the SYSCTL. Since the **IND** display is a 35-segment display, this test indicates all segments are working.

---

32 Release the **ACO TEST** push-button on the LNW2 SYSCTL when the red rectangle disappears in the **IND** display.

Result: The current software generic appears in the **IND** display on the LNW2 SYSCTL and the shelf LEDs return to their previous status.

---

33 From the Network View of the *WaveStar*® CIT session you established in Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218), select the **View:** pull-down menu and select **CIT OSI Neighbors**.

Important! This **View:** is not the menu bar item View → ...; it is located above the NE Name pull-down menu.

---

34 From the Network View, select **View** → **Refresh OSI View**.

Result: The CIT OSI neighbor(s) are automatically detected.

Your TID is your original TID, the same TID provisioned on your 5.1.xNE.

---

35 In the Network View, right-click the NE icon that was detected, and select **Graphical Using** → **OSI** from the resulting menu.

Result: The *System Type Selection* window appears.

---

36 In the *System Type Selection* window, select DMX and click **OK**.

Result: The *NE Login Dialog* window appears.

---

37 In the NE login window, login to the shelf using your original user ID and password.

Click **OK**.

Result: The title bar of the System View and the legal notice text both reflect the current NE software generic, for example: 9.1.0.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

---

38 Is the Generic Software Version correct?

If...	Then...
Yes	STOP! End of Procedure.
No	Contact your next level of support.

END OF STEPS

Procedure 6-19.3: Upgrade software generic via FTAM (7.1.x, 8.0.x, 9.0.1 or later to 9.1.x)

Overview

Use this procedure to download the software generic via the File Transfer and Access Management (FTAM) protocol from the *WaveStar*® CIT to the local network element or a remote network element via DCC with OSI connectivity to the network element. To download the software generic to a local shelf via FTP, refer to Procedure 6-17: "Upgrade software generic via FTP" (p. 6-175). To download the software generic to a remote shelf via FTTD, refer to Procedure 6-18: "Upgrade software generic via FTTD" (p. 6-212).

Important! Your NE must be running Release 7.1.x, 8.0.x, or 9.0.1 or later to use this procedure.

Required equipment

Refer to "Required equipment" (p. 6-218) in Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure, complete Procedure 6-19: "Upgrade software generic via FTAM" (p. 6-218).

Steps

Complete the following steps to download and upgrade system software via FTAM.

1 Before upgrading the network, perform a backup the NE database.

Reference: Procedure 6-23: "Backup and restore NE database via FTAM" (p. 6-279)

2 From the System View menu, select **Configuration** → **Software** → **Download Software**.

Result: The *Download Software* window appears.

3 In the pull-down **Download From/Via:** menu, select **FTAM**.

4 In the **Source/Destination Directory Path** panel, enter the current location of the generic to be downloaded or use the **Browse** button (if available) to select the generic to be downloaded.

Important! If you selected the default installation location for the *WaveStar®* CIT and software generic: **`\generics\DMX\9.1.x\p`**. If necessary, replace 9.1.0 with your current release, for example 9.1.1. The *WaveStar®* CIT automatically populates the FTAM Responder and NSAP fields.

The value of the Path field can be either an absolute path or a relative path that is relative to the FTAM server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: **`C:\Program Files\Alcatel-Lucent\WaveStar CIT\generics\DMX\9.1.x\p`**. If you had an older *WaveStar®* CIT installed prior to installing the current *WaveStar®* CIT, your path could start with C:\Program Files\Lucent Technologies\. The syntax of the relative path must start with the path name; for example: **`\generics\DMX\9.1.x\p`**. If necessary, replace 9.1.0 with your current release, for example 9.1.1.

5 In the **Product Type** panel, select the product type of the software generic that you are downloading (not necessarily the same as the NE to which you are downloading).

6 Click **OK**.

Result: A warning message appears asking you to confirm executing this command. Verify the information and click **Yes**.

While the download is in progress (approximately 30 minutes), a progress indicator window is present.

The download can be cancelled any time by pressing the **Cancel** button on the progress screen.

When the transfer is complete, the *Progress Indicator* window closes and the download software successful window appears. Click **OK**.

7 **Important!** Do NOT insert a new circuit pack in the shelf until after you apply the new software generic and clear the `dormant/exec version mismatch` condition.

Do you wish to apply (activate) the software generic that you recently downloaded to the dormant area of the Alcatel-Lucent 1665 DMX shelf?

If...	Then...
Yes	Proceed to Procedure 6-20: "Apply software generic" (p. 6-249) and then continue with Step 8.
No	Continue with Step 8.

8 Do you wish to upgrade additional shelves via FTAM?

If...	Then...
Yes	Repeat this procedure from Step 2 for each shelf that you wish to upgrade via FTAM.
No	STOP! End of Procedure.

END OF STEPS

Procedure 6-20: Apply software generic

Overview

Use this procedure to apply (activate) a software generic currently in the Dormant area of an NVM in the LNW2.

Privilege level

You must log in as a Privileged user to complete this procedure.

Before you begin

Before performing this procedure,

- Refer to “Before you begin” (p. 6-3) and “Required equipment” (p. 6-3) in this chapter.
- Ensure that no loopbacks exist on the shelf.
  1. Select **View** → **Loopback** from the System View menu. Select **Shelf** from the View Loopbacks window, then click **Select**.

     Print or save the existing loopbacks to be released, then click **Close**.
  2. Select **Fault** → **Analysis** → **Loopback** from the System View menu. Expand the details in the Loopback window, select the port with the loopback to be released, then click **Select**. Select Release and the Loopback Type, then click **Apply** at the bottom of the Loopback window. Click **Yes** to the Warning message to release the loopback. Click **Close** to exit.

Important! Do *NOT* insert circuit packs into the shelf until after the apply is complete. The apply is not complete if the Alarm List contains either a `dormant/exec code mismatch` or a `waiting for download` condition. Waiting for download indicates that there is at least one circuit pack that requires a firmware upgrade.

Steps

Complete the following steps to apply (activate) a Dormant or Previous software generic.

1 From the System View menu, select **Configuration** → **Software** → **Apply Software**.

Result: The *Apply Software* window appears.

2 Select and/or enter the following information in the *Apply Software* window:

1. From the **Available Generics** panel, select the software generic (Previous or Dormant) to be activated.
2. From the **Activation Scheduling** panel, you can schedule the activation time and date in *one* of the following ways:
   - Select **Install Immediately**. The software installs as soon as possible after you click **OK** and accept the warning screen.

     This installation option cannot be cancelled.
   - Select **Install In 15 Minutes**. The software installs 15 minutes after you click **OK**.
   - Select **Specify Install Date/Time** and select the **Year**, **Month**, **Date**, and **Time**.

   You can provision the time format display for your *WaveStar*® CIT from the Network View by selecting **View** → **Preferences** and clicking the Display tab. This screen allows you to choose your preference for time format, either a 12-hour clock or a 24-hour clock.
   - If your time format preference is a 12-hour clock, select **Hour:** (0–12), **Minutes:** (0–59), and **Seconds:** (0–59) from the pull-down menus. You must also specify am or pm by selecting one of the radio buttons.
   - If your time format preference is a 24-hour clock, select the **Hour:** (0–23), **Minutes:** (0–59), and **Seconds:** (0–59) from the pull-down menus.
3. From the **Apply Type** panel, select one of the following Types:
   - **Smart** (default): Upgrades the SYSCTL and smart circuit packs if the version of software on the circuit pack is different from the version of the dormant software generic.

     If the upgrade affects service on a smart OLIU circuit pack, the software apply (activation) command is denied.
   - **Smart, Override Alarms**: Upgrades the SYSCTL and smart circuit packs if the version of software on the circuit pack is different from the version of the dormant software generic.

     This also includes service-affecting upgrades to smart OLIU circuit packs.
4. Click **OK**.

   A warning message appears asking you to confirm the execution of this command.
5. Click **OK** to continue or **Cancel** to return to the *Apply Software* screen.

   While the Apply is in progress, two conditions appear in the Alarm List, `install program IP` (software is installing) and `generic validation IP` (the generic and the databases on the NVMs are being compared).

Important! You can cancel a scheduled apply that was scheduled by selecting either *Install In 15 Minutes* or *Specify Install Date/Time* any time before the software applies. Select **Configuration** → **Software** → **Apply Software** menu, select the generic that is scheduled to install, select **Cancel Install**, and then click **OK**.

3 Approximately 15 minutes after the scheduled apply time, the apply is complete.

A flashing **b** in the **IND** display on the SYSCTL indicates that a boot is in progress.

When the confirmation screen appears, click **OK**.

Result: The *System View* closes.

4 Establish a *WaveStar*® CIT session (depending on the physical connection used) and log in again to your Alcatel-Lucent 1665 DMX shelf.

Result: The title bars of the *System View* and the legal notice both reflect the current NE software generic, for example 9.1.0.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

5 Is the Generic Software Version correct?

If...	Then...
Yes	The generic was successfully installed on the SYSCTL. If necessary, the firmware on the smart circuit packs is now upgraded. In the Alarm List, the `waiting for download` condition is present for the circuit packs that are waiting for their firmware to be upgraded. STOP! End of Procedure.
No	Contact your next level of support.

END OF STEPS

Procedure 6-21: Backup and restore NE database via FTP

Overview

Use this procedure to backup and restore the NE database or to set up an automatic backup schedule via FTP.

Important! You must have direct TCP/IP connectivity to your NE and the NE must have a defined IP address.

Privilege level

You must log in as a Privileged user to complete this procedure.

Required equipment

In addition to "Required equipment" (p. 6-3) listed in this chapter, CAT5 Ethernet cable with either a 10/100 hub or a cross-over cable for the **LAN** or **IAO LAN** port (required for TCP/IP connectivity) is also required.

Before you begin

Before performing this procedure,

1. Refer to "Before you begin" (p. 6-3) and "Required equipment" (p. 6-3)in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

The *WaveStar®* CIT is not a fully implemented FTP server, but it can handle backup and restore capabilities. For automatic backups, OMS or another large capacity FTP server can be used. The *WaveStar®* CIT is *not* recommended for automatic backups.

The backup feature can be forced or scheduled to complete automatically at specified intervals.

If you log in via TCP/IP, your PC must be part of the GNE's TCP/IP Gateway Host List. Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* for more information.

Important! If the FTP server associated with the *WaveStar®* CIT fails to start, it could mean that another program using an FTP server is already running. Depending on what operating system you are using, you must go to the device file and disable the FTP server. Refer to Procedure 6-25: "Disable an FTP server on your PC" (p. 6-287) for instructions for each allowed operating system.

Steps

Complete the following steps to backup and restore the system.

1 Connect the PC and establish a *WaveStar*® CIT session with the gateway NE.

Important! You must have direct TCP/IP connectivity to your NE and the NE must have a defined IP address.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

2 From the System View menu, select **Administration** → **Set NE** and enable **File Transfer Protocol**.

3 Click **OK**.

4

If...	Then...
performing an immediate system backup,	Proceed to Procedure 6-21.1: "Backup NE database via FTP" (p. 6-254).
scheduling or discontinuing an automatic system backup,	Proceed to Procedure 6-21.2: "Provision automatic database backup schedule via FTP" (p. 6-257).
performing a system restore,	Proceed to Procedure 6-21.3: "Restore NE database via FTP" (p. 6-261).

END OF STEPS

Procedure 6-21.1: Backup NE database via FTP

Overview

Use this procedure to backup the NE database via FTP.

Important! You must have direct TCP/IP connectivity to your NE and the NE must have a defined IP address.

Required equipment

Refer to “Required equipment” (p. 6-252) in Procedure 6-21: “Backup and restore NE database via FTP” (p. 6-252) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure, complete Procedure 6-21: “Backup and restore NE database via FTP” (p. 6-252).

Steps

Complete the following steps to backup the NE database via FTP.

1 From the System View menu, select **Configuration** → **Software** → **Remote Backup**.

2 In the pull-down **Backup To/Via:** menu, select **FTP**.

3 Select the connection from the **Profile** pull-down menu and proceed to Step 5. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user ID/password can be different.)

4 If you entered connection information in Step 3 and wish to keep the information for future backups:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

   Entries to the **Profile** pull-down menu can be changed using the **Modify**, **Apply**, and **Save** buttons or removed using the **Delete** button.

5 In the **Source/Destination Directory Path** field, enter **`\backups\<filename>`** if you wish to save the backup file to the default location. (If the *WaveStar*® CIT is the FTP server, a maximum of 80 characters is suggested for this field.)

You can also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and over-write the default entry. The **Browse** button is not available (greyed out) if the FTP server is not the local *WaveStar*® CIT or the IP address of the FTP server is not in the same subnet as the IP address of the shelf.

> **Important!** The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.
>
> The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is
>
> `C:\Program Files\Alcatel-Lucent\WaveStar CIT\`
>
> If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, the path could start with C:\Program Files\Lucent Technologies\.
>
> If you wish to store your data in a subdirectory, enter **`\backups\<subdirectory>\<filename>`** if the subdirectory exists before the command is sent. If any directory in the path does not exist, the command is denied because this command does not create directories.

6 Click **OK**.

You are asked to verify that you wish to backup to the directory that you entered. Click **Yes** if you typed the path correctly.

Result: The *Progress Indicator* screen appears, indicating that the backup is in progress. When the backup completes, a `Remote Backup successful` screen appears. Click **OK**. The backup file is now stored. If the default path and a subdirectory were used, the file can be found at:

`C:\Program Files\Alcatel-Lucent\\WaveStar CIT\backups\`
`<subdirectory>\<filename>`

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, the path could start with C:\Program Files\Lucent Technologies\.

END OF STEPS

Procedure 6-21.2: Provision automatic database backup schedule via FTP

Overview

Use this procedure to provision an automatic backup schedule via FTP.

Required equipment

Refer to "Required equipment" (p. 6-252) in Procedure 6-21: "Backup and restore NE database via FTP" (p. 6-252) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure, complete Procedure 6-21: "Backup and restore NE database via FTP" (p. 6-252).

Steps

Complete the following steps to provision an automatic backup schedule.

1 From the System View menu, select **Configuration** → **Software** → **Configure Auto Backup Interval**.

Important! If the *WaveStar*® CIT is guaranteed to be available (connected and running) at all scheduled backup times, the *WaveStar*® CIT can serve as an FTP server. OMS or another large capacity FTP server can also be used.

2 From the *Configure Auto Backup* screen, select the **Files** tab at the top of the screen.

3 In the pull-down **Backup To/Via:** menu, select **FTP**.

4 Select the connection from the **Profile** pull-down menu and then proceed to Step 6. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user ID/password can be different.)

5 If you entered connection information in Step 4 (rather than selected an established profile), assign a new profile name to this information to allow Automatic Backup to store the FTP login password. To assign a new profile name:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

   Entries to the **FTP Profile** pull-down menu can be changed using the **Modify**, **Apply**, and **Save** buttons *or* removed using the **Delete** button.

6 In the **File Path:** field, enter **`\backups\<filename>`** if you wish to save the backup file to the default location. (If the *WaveStar*® CIT is the FTP server, a maximum of 80 characters is suggested for this field.)

You can also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and over-write the default entry. The **Browse** button is not available (greyed out) if the FTP server is not the local *WaveStar*® CIT or the IP address of the FTP server is not in the same subnet as the IP address of the shelf.

Important! The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.

The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is

```
C:\Program Files\Alcatel-Lucent\WaveStar CIT\
```

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, the path could start with C:\Program Files\Lucent Technologies\.

If you wish to store your data in a subdirectory, enter **`\backups\<subdirectory>\<filename>`** if the subdirectory exists before the command is sent. If any directory in the path does not exist, the command is denied because this command does not create directories.

7 From the **Type:** menu in the **Backup Type** panel, select **Forced** from the pull-down menu. *NOTE: No other options are available at this time.*

8 From the **Files:** menu in the **Number Of Files** panel, select a number from 1 to 9 (default is 2) from the pull-down menu, which indicates the number of backup files to be stored automatically before the files begin to overwrite.

Once established, the filename that you supplied in Step 6 is appended with “1” (FILENAME1). In subsequent backups, the “1” increases by one until the number selected in this step is reached; then the files begins overwriting beginning with FILENAME1.

9 Select the **Schedule** tab at the top of the screen.

10 From the **Days** menu in the **Update Interval** panel, select a number from 1 to 99 (default is 30), which indicates the number of days between automatic backups. Select the number by sliding the arrow over the scale until the desired number appears in the field.

Important! Setting this field to “0” cancels automatic backup.

11

If you...	Then...
wish to provision a start date and start time for the automatic backup,	Perform the following to provision the start date: 1. Select **Specify Date** in the **Backup Start Date/Time** panel, 2. Select the **Year:** and **Month:** from the pull-down menus 3. Select a day from the calendar. Proceed to Step 12 to provision the start time.
wish to only provision the start time for the automatic backup,	Proceed to Step 12 to provision the start time.
do not wish to provision the start date or start time for the automatic backup,	Proceed to Step 13. The first backup begins immediately upon completion of this procedure and the next backup begins after the requested number of days.

12 To provision a start time for the automatic backup:

1. Select **Specify Time** in the **Backup Start Date/Time** panel,
2. You can provision the time format display for your *WaveStar*® CIT from the Network View by selecting **View** → **Preferences** and clicking the Display tab. This screen allows you to choose your preference for time format, either a 12-hour clock or a 24-hour clock.
   - If your time format preference is a 12-hour clock, select **Hour:** (0–12), **Minutes:** (0–59), and **Seconds:** (0–59) from the pull-down menus. You must also specify am or pm by selecting one of the radio buttons.
   - If your time format preference is a 24-hour clock, select the **Hour:** (0–23), **Minutes:** (0–59), and **Seconds:** (0–59) from the pull-down menus.

   It is recommended that only one backup occur at a time for the CIT. However, larger servers can be able to handle multiple backups at the same time. Network backups should be performed a few minutes apart.

13 Click **OK**.

A warning screen appears, indicating that execution of provision can temporarily affect service. Select **Yes**.

END OF STEPS

Procedure 6-21.3: Restore NE database via FTP

Overview

Use this procedure to restore the NE database using FTP.

Required equipment

Refer to “Required equipment” (p. 6-252) in Procedure 6-21: “Backup and restore NE database via FTP” (p. 6-252) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure, complete Procedure 6-21: “Backup and restore NE database via FTP” (p. 6-252).

Steps

Complete the following steps to restore the NE database via FTP.

1

NOTICE

Service-disruption hazard

Restoring the network element database can be service-affecting.

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

From the System View menu, select **Configuration** → **Software** → **Remote Restore**.

Important! If the TID has changed since the backup was performed, then the restore is denied. The software release of the backup database must be the same as the current software generic. In addition, if any service-related parameters (for example, cross-connections) have been changed since the last backup file was created, those changes are lost and service can be affected. These changes must be reentered.

2 In the pull-down **Restore From/Via:** menu, select **FTP**.

3 Select the connection from the **Profile** pull-down menu and then proceed to Step 5. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user ID/password can be different.)

4 If you entered connection information in Step 3 and wish to keep the information for future restores:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

Entries to the **Profile** pull-down menu can be changed using the **Modify**, **Apply**, and **Save** buttons or removed using the **Delete** button.

5 In the **Source/Destination Directory Path** panel, enter the location where the database information is stored. Enter the path and filename exactly as it was entered in Procedure 6-21.1: "Backup NE database via FTP" (p. 6-254) or Procedure 6-21.2: "Provision automatic database backup schedule via FTP" (p. 6-257) (For example: **`\backups\<subdirectory>\<filename>`**).

You can also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and over-write the default entry. The **Browse** button is not available (greyed out) if the FTP server is not the local *WaveStar*® CIT or the IP address of the FTP server is not in the same subnet as the IP address of the shelf.

Important! The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.

The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is

```
C:\Program Files\Alcatel-Lucent\WaveStar CIT\
```

If you had an older *WaveStar®* CIT installed prior to installing the current *WaveStar®* CIT, the path could start with C:\Program Files\Lucent Technologies\.

6 Click **OK**.

You are asked to verify that you wish to restore from the directory that you entered. Click **Yes** if you typed the path correctly.

A second warning screen appears that states that Execution of RESTORE causes a System Reset. Click **Yes**.

Result: The *Progress Indicator* screen appears, indicating that the restore is in progress. When the restore is complete, a *WaveStar®* CIT warning screen appears, stating *NE reset after successful restore, CIT is going to log out*.

7 Click **OK**.

Result: A second *WaveStar®* CIT warning screen appears, stating *Communication to network element is lost, system view will now be closed.*

8 Click **OK**.

END OF STEPS

Procedure 6-22: Backup and restore NE database via FTTD

Overview

Use this procedure to backup and restore the NE database or to set up an automatic backup schedule via FTAM-FTP gateway or file transfer translation device (FTTD) for a remote NE without direct TCP/IP connectivity.

Privilege level

You must login as a Privileged user to complete this procedure.

Required equipment

In addition to "Required equipment" (p. 6-3) listed in this chapter, CAT5 Ethernet cable with either a 10/100 hub or a cross-over cable for the **LAN** or **IAO LAN** port (required for TCP/IP connectivity) is also required.

Before you begin

Before performing this procedure,

1. Refer to "Before you begin" (p. 6-3) and "Required equipment" (p. 6-3) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Alcatel-Lucent 1665 DMX can also act as an FTAM-FTP gateway or file transfer translation device (FTTD). The FTTD allows Alcatel-Lucent 1665 DMX to function as a gateway network element (GNE) that facilitates file downloads between FTP servers and remote network elements (RNEs) connected to the Alcatel-Lucent 1665 DMX.

This procedure uses FTP (file transfer protocol) and FTAM (file transfer and access management) to backup and restore all Alcatel-Lucent 1665 DMX provisionable data on a shelf.

The *WaveStar®* CIT is not a fully implemented FTP server, but it can handle backup and restore capabilities. For automatic backups, OMS or another large capacity FTP server can be used. The *WaveStar®* CIT is *not* recommended for automatic backups.

The backup feature can be forced or scheduled to complete automatically at specified intervals.

If you log in via TCP/IP, your PC must be part of the GNE's TCP/IP Gateway Host List. Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* for more information.

Important! If the FTP server associated with the *WaveStar*® CIT fails to start, it could mean that another program using an FTP server is already running. Depending on what operating system you are using, you must go to the device file and disable the FTP server. Refer to Procedure 6-25: "Disable an FTP server on your PC" (p. 6-287) for instructions for each allowed operating system.

Steps

Complete the following steps to backup and restore the system.

1 Connect the PC and establish a *WaveStar*® CIT session to the gateway Network Element.

Important! You must have direct TCP/IP connectivity to your NE and the NE must have a defined IP address.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

2 From the System View menu, select **Administration** → **Set NE** and enable **File Transfer Protocol (FTP)** and FTAM-FTP (FTTD) Gateway Control.

3 Click **OK**.

4 Is your remote NE in the same OSI network as your gateway NE?

If	Then
Yes	Proceed to Step 6.
No	Continue with Step 5.

5 From the System View, select **Administration** → **Data Communications**.

Select the **Network Layer** tab and record the NSAP from the **Network Service Access Point** panel (the NSAP is a 40-digit hex number). This NSAP is required later in this procedure.

6 Establish a *WaveStar*® CIT session to the remote Network Element.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

7

If...	Then...
performing an immediate system backup,	Proceed to Procedure 6-22.1: "Backup NE database via FTTD" (p. 6-267).
scheduling or discontinuing an automatic system backup,	Proceed to Procedure 6-22.2: "Provision automatic database backup schedule via FTTD" (p. 6-270).
performing a system restore,	Proceed to Procedure 6-22.3: "Restore NE database via FTTD" (p. 6-275).

END OF STEPS

Procedure 6-22.1: Backup NE database via FTTD

Overview

Use this procedure to backup the NE database via FTAM-FTP gateway or file transfer translation device (FTTD) for a remote NE without direct TCP/IP connectivity.

Required equipment

Refer to "Required equipment" (p. 6-264) in Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure, complete Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264).

Steps

Complete the following steps to backup the NE database via FTTD.

1 From the System View menu, select **Configuration** → **Software** → **Remote Backup** .

2 In the pull-down **Backup To/Via:** menu, select **FTTD** and verify that the **FTTD** tab is selected.

3 Define the FTAM-FTP Gateway in one of the following ways:

- If the TID of the FTAM-FTP Gateway has been previously defined, select it from the **TID** pull-down menu.
  OR
- If the gateway NE and the remote NE are in the same OSI area:
  1. Enter the TID of the FTAM-FTP Gateway in the **TID** field and click **Get NSAP**. (If any fields on this screen are populated, click **Clear** before you enter the TID.)
  2. Click **Add** and then **Save**. The TID is added to the pull-down menu for this CIT. If you replace the SYSCTL in the GNE, re-enter the NSAP address for this gateway NE's TID.

  OR

- If the gateway NE and the remote NE are *not* in the same OSI area:
    1. In the **FTTD** panel, select **_template_** from the **TID:** pull-down, which pre-populates most of the fields on this form (required value for **Psel** is 02, **Ssel** is 5353, and **Tsel** is 5454).
    2. Click **Modify**.
    3. Replace **_template_** with the TID of the FTAM-FTP gateway NE.
    4. Edit the NSAP Address fields as required. Refer to Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264), Step 5.
    5. Verify that the Selector (**Sel:**) field is "1d" .
    6. Click **Add** and then **Save**. The TID has been added to the pull-down menu for this CIT. If you replace the SYSCTL in the GNE, re-enter the NSAP address for this GNE's TID.

4 Select the **FTP** tab.

5 Select the connection from the **Profile** pull-down menu and then proceed to Step 7. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user ID/password can be different.)

6 If you entered connection information in Step 5 and wish to keep the information for future backups:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

    Important! Entries to the **FTP Profile** pull-down menu can be changed using the **Modify**, **Apply**, and **Save** buttons or removed using the **Delete** button.

7 In the **Source/Destination Directory Path** field, enter **`\backups\<filename>`**. (If the *WaveStar*® CIT is the FTP server, a maximum of 80 characters is suggested for this field.)

You can also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and over-write the default entry. The **Browse** button is not available (greyed out) if the FTP server is not the local *WaveStar*® CIT or the IP address of the FTP server is not in the same subnet as the IP address of the shelf.

Important! The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.

The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is

`C:\Program Files\Alcatel-Lucent\WaveStar CIT\`

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, the path could start with C:\Program Files\Lucent Technologies\.

If you wish to store your data in a subdirectory, enter **`\backups\<subdirectory>\<filename>`** if the subdirectory exists before the command is sent. If any directory in the path does not exist, the command is denied because this command does not create directories.

---

8 Click **OK**.

You are asked to verify that you wish to backup to the directory that you entered. Click **Yes** if you typed the path correctly.

Result: The *Progress Indicator* screen appears, indicating that the backup is in progress. When the backup completes, a `Remote Backup successful` screen appears. Click **OK**. The backup file is now stored. If the default path and a subdirectory were used, the file can be found at:

```
C:\Program Files\Alcatel-Lucent\\WaveStar CIT\backups\
<subdirectory>\<filename>
```

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, the path could start with C:\Program Files\Lucent Technologies\.

END OF STEPS

Procedure 6-22.2: Provision automatic database backup schedule via FTTD

Overview

Use this procedure to provision an automatic backup schedule via FTAM-FTP gateway or file transfer translation device (FTTD) for a remote NE without direct TCP/IP connectivity.

Required equipment

Refer to “Required equipment” (p. 6-264) in Procedure 6-22: “Backup and restore NE database via FTTD” (p. 6-264) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure, complete Procedure 6-22: “Backup and restore NE database via FTTD” (p. 6-264).

Steps

Complete the following steps to provision an automatic backup schedule via FTTD.

1. From the System View menu, select **Configuration** → **Software** → **Configure Auto Backup Interval** .

   Important! If the *WaveStar*® CIT is guaranteed to be available (connected and running) at all scheduled backup times, the *WaveStar*® CITcan serve as an FTP server. OMS or another large capacity FTP server can also be used.

2. From the **Configure Auto Backup** screen, and select the **Files** tab at the top of the screen.

3. In the pull-down **Backup To/Via:** menu, select **FTTD** and select the **FTTD** tab.

4. Define the FTAM-FTP Gateway in **one** of the following ways:

   - If the TID of the FTAM-FTP Gateway has been previously defined, select it from the **TID** pull-down menu.

OR

- If the gateway NE and the remote NE are in the same OSI area:
  1. Enter the TID of the FTAM-FTP Gateway in the **TID** field and click **Get NSAP**. (If any fields on this screen are populated, click **Clear** before you enter the TID.)
  2. Click **Add** and then **Save**. The TID is added to the pull-down menu for this CIT. If you replace the SYSCTL in the GNE, re-enter the NSAP address for this gateway NE's TID.

  OR
- If the gateway NE and the remote NE are *not* in the same OSI area:
  1. In the **FTTD** panel, select **_template_** from the **TID:** pull-down, which pre-populates most of the fields on this form (required value for **Psel** is 02, **Ssel** is 5353, and **Tsel** is 5454).
  2. Click **Modify**.
  3. Replace **_template_** with the TID of the FTAM-FTP gateway NE.
  4. Edit the NSAP Address fields as required. Refer to Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264), Step 5.
  5. Verify that the Selector (**Sel:**) field is "1d" .
  6. Click **Add** and then **Save**. The TID has been added to the pull-down menu for this CIT. If you replace the SYSCTL in the GNE, re-enter the NSAP address for this GNE's TID.

5 Select the **FTP** tab.

6 Select the connection from the **Profile** pull-down menu and then proceed to Step 8. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however, your user ID/password can be different.)

7 If you entered connection information in Step 6 (rather than selected an established profile), should assign a new profile name to this information to allow Automatic Backup to store the FTP login and password. To assign a new profile:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

   Entries to the **FTP Profile** pull-down menu can be changed using the **Modify**, **Apply**, and **Save** buttons *or* removed using the **Delete** button.

8 In the **File Path:** field, enter **\backups\<filename>**. (If the *WaveStar*® CIT is the FTP server, a maximum of 80 characters is suggested for this field.)

You can also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and over-write the default entry. The **Browse** button is not available (greyed out) if the FTP server is not the local *WaveStar*® CIT or the IP address of the FTP server is not in the same subnet as the IP address of the shelf.

Important! The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.

The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is

```
C:\Program Files\Alcatel-Lucent\WaveStar CIT\
```

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, the path could start with C:\Program Files\Lucent Technologies\.

If you wish to store your data in a subdirectory, enter **\backups\<subdirectory>\<filename>** if the subdirectory exists before the command is sent. If any directory in the path does not exist, the command is denied because this command does not create directories.

9 From the **Type:** menu in the **Backup Type** panel, select **Forced** from the pull-down menu. *NOTE: No other options are available at this time.*

10 From the **Files:** menu in the **Number Of Files** panel, select a number from 1 to 9 (default is 2) from the pull-down menu, which indicates the number of backup files to be stored automatically before the files begin to overwrite.

Once established, the filename that you supplied in Step 8 is appended with "1" (FILENAME1). In subsequent backups, the "1" increases by one until the number selected in this step is reached; then the files begins overwriting beginning with FILENAME1.

11 Select the **Schedule** tab at the top of the screen.

12 From the **Days** menu in the **Update Interval** panel, select a number from 1 to 99 (default is 30), which indicates the number of days between automatic backups. The number can be selected by sliding the arrow over the scale until the desired number appears in the field.

Important! Setting this field to "0" cancels automatic backup.

13

If you...	Then...
wish to provision a start date and start time for the automatic backup,	Perform the following to provision the start date: 1. Select **Specify Date** in the **Backup Start Date/Time** panel, 2. Select the **Year:** and **Month:** from the pull-down menus 3. Select a day from the calendar. Proceed to Step 14 to provision the start time.
wish to only provision the start time for the automatic backup,	Proceed to Step 14 to provision the start time.
do not wish to provision the start date or start time for the automatic backup,	Proceed to Step 15. The first backup begins immediately upon completion of this procedure and the next backup begins after the requested number of days.

14 To provision a start time for the automatic backup:

1. Select **Specify Time** in the **Backup Start Date/Time** panel,
2. You can provision the time format display for your *WaveStar*® CIT from the Network View by selecting **View** → **Preferences** and clicking the Display tab. This screen allows you to choose your preference for time format, either a 12-hour clock or a 24-hour clock.
   - If your time format preference is a 12-hour clock, select **Hour:** (0–12), **Minutes:** (0–59), and **Seconds:** (0–59) from the pull-down menus. You must also specify am or pm by selecting one of the radio buttons.
   - If your time format preference is a 24-hour clock, select the **Hour:** (0–23), **Minutes:** (0–59), and **Seconds:** (0–59) from the pull-down menus.

   It is recommended that only one backup occur at a time for the CIT. However, larger servers can be able to handle multiple backups at the same time. Network backups should be performed a few minutes apart.

15 Click **OK**.

A warning screen appears, indicating that execution of provision can temporarily affect service. Select **Yes**.

END OF STEPS

Procedure 6-22.3: Restore NE database via FTTD

Overview

Use this procedure to restore the NE database via FTAM-FTP gateway or file transfer translation device (FTTD) for a remote NE without direct TCP/IP connectivity.

Required equipment

Refer to "Required equipment" (p. 6-264) in Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure, complete Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264).

Steps

Complete the following steps to restore the NE database via FTAM-FTP gateway or file transfer translation device (FTTD).

1 **NOTICE**

Service-disruption hazard

Restoring the network element database can be service-affecting.

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

From the System View menu, select **Configuration** → **Software** → **Remote Restore**.

Important! If the TID has changed since the backup was performed, then the restore is denied. The software release of the backup database must be the same as the current software generic. In addition, if any service-related parameters (for example, cross-connections) have been changed since the last backup file was created, those changes are lost and service can be affected. These changes must be reentered.

2 In the pull-down **Restore From/Via:** menu, select **FTTD** and select the **FTTD** tab.

3 Define the FTAM-FTP Gateway in one of the following ways:

- If the TID of the FTAM-FTP Gateway has been previously defined, select it from the **TID** pull-down menu.

OR

- If the gateway NE and the remote NE are in the same OSI area:
  1. Enter the TID of the FTAM-FTP Gateway in the **TID** field and click **Get NSAP**. (If any fields on this screen are populated, click **Clear** before you enter the TID.)
  2. Click **Add** and then **Save**. The TID is added to the pull-down menu for this CIT. If you replace the SYSCTL in the GNE, re-enter the NSAP address for this gateway NE's TID.

  OR
- If the gateway NE and the remote NE are *not* in the same OSI area:
  1. In the **FTTD** panel, select **_template_** from the **TID:** pull-down, which pre-populates most of the fields on this form (required value for **Psel** is 02, **Ssel** is 5353, and **Tsel** is 5454).
  2. Click **Modify**.
  3. Replace **_template_** with the TID of the FTAM-FTP gateway NE.
  4. Edit the NSAP Address fields as required. Refer to Procedure 6-22: "Backup and restore NE database via FTTD" (p. 6-264), Step 5.
  5. Verify that the Selector (**Sel:**) field is "1d" .
  6. Click **Add** and then **Save**. The TID has been added to the pull-down menu for this CIT. If you replace the SYSCTL in the GNE, re-enter the NSAP address for this GNE's TID.

4 Select the **FTP** tab.

5 Select the connection from the **Profile** pull-down menu and then proceed to Step 7. *OR* Enter information for a new profile as follows:

1. In the **Server** panel, select **IP** and enter the address of the FTP server. (If the *WaveStar*® CIT is the FTP server, you can determine its IP address by entering **`ipconfig`** from the **MS DOS** prompt on your PC.)
2. If necessary, enter the port (default is blank). Defining the port is not required for the backup to execute successfully. However, a value of 21 is valid if entered.
3. In the **User** panel, enter the user name and password for the FTP server. (If you are using the *WaveStar*® CIT as your FTP server, the default user name/password for the *WaveStar*® CIT is **`LUC01`**/**`LUC+01`**, however your user ID/password can be different.)

6 If you entered connection information in Step 5 and wish to keep the information for future restores:

1. Type a new name in the **Profile** menu.
2. Click **Add** to add the profile to the list.
3. Click **Save** to save the list.

Important! Entries to the **FTP Profile** pull-down menu can be changed using the **Modify**, **Apply**, and **Save** buttons or removed using the **Delete** button.

7 In the **Source/Destination Directory Path** panel, enter the location where the database information is stored. Enter the path and filename exactly as it was entered in Procedure 6-22.1: “Backup NE database via FTTD” (p. 6-267) or Procedure 6-22.2: “Provision automatic database backup schedule via FTTD” (p. 6-270). For example: **`\backups\<subdirectory>\<filename>`**.

You can also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and over-write the default entry. The **Browse** button is not available (greyed out) if the FTP server is not the local *WaveStar*® CIT or the IP address of the FTP server is not in the same subnet as the IP address of the shelf.

Important! The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.

The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is

```
C:\Program Files\Alcatel-Lucent\WaveStar CIT\
```

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, the path could start with C:\Program Files\Lucent Technologies\.

8 Click **OK**.

You are asked to verify that you wish to restore from the directory that you entered. Click **Yes** if you typed the path correctly.

A second warning screen appears that states that Execution of RESTORE causes a System Reset. Click **Yes**.

Result: The *Progress Indicator* screen appears, indicating that the restore is in progress. When the restore is complete, a *WaveStar*® CIT warning screen appears, stating *NE reset after successful restore, CIT is going to log out*.

9 Click **OK**.

Result: A second *WaveStar*® CIT warning screen appears, stating *Communication to network element is lost, system view will now be closed.*

10 Click **OK**.

END OF STEPS

Procedure 6-23: Backup and restore NE database via FTAM

Overview

Use this procedure to backup and restore the local NE database via the File Transfer and Access Management (FTAM) protocol. Scheduled automatic backups are not supported using FTAM.

Privilege level

You must log in as a Privileged user to complete this procedure.

Required equipment

In addition to "Required equipment" (p. 6-3) listed in this chapter, CAT5 Ethernet cable with either a 10/100 hub or a cross-over cable for the **LAN** or **IAO LAN** port (required for TCP/IP connectivity) is also required.

Before you begin

Before performing this procedure,

1. Refer to "Before you begin" (p. 6-3) and "Required equipment" (p. 6-3) in this chapter.
2. Refer to "Electrostatic discharge" (p. 1-26) in Chapter 1, "Safety".

Steps

Complete the following steps to backup and restore the system.

1 Connect the PC and establish a *WaveStar*® CIT session to the local Network Element that is to be backed up or restored.

Important! You must login via OSI.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

2

If...	Then...
performing an immediate system backup,	Proceed to Procedure 6-23.1: "Backup NE database via FTAM" (p. 6-281).
performing a system restore,	Proceed to Procedure 6-23.2: "Restore NE database via FTAM" (p. 6-283).

END OF STEPS

Procedure 6-23.1: Backup NE database via FTAM

Overview

Use this procedure to backup the local NE database or a remote NE database (with DCC connectivity) via the File Transfer and Access Management (FTAM) protocol to the *WaveStar*® CIT.

Required equipment

Refer to “Required equipment” (p. 6-279) in Procedure 6-23: “Backup and restore NE database via FTAM” (p. 6-279) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure, complete Procedure 6-23: “Backup and restore NE database via FTAM” (p. 6-279).

Steps

Complete the following steps to backup an NE database using FTAM.

1 From the System View menu, select **Configuration** → **Software** → **Remote Backup**.

2 In the pull-down **Backup To/Via:** menu, select **FTAM**.

3 In the **Source/Destination Directory Path** field, enter **`\backups\<filename>`**.

You can also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and over-write the default entry.

> **Important!** The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.
>
> The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is
>
> `C:\Program Files\Alcatel-Lucent\WaveStar CIT\`
>
> If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, the path could start with C:\Program Files\Lucent Technologies\.

If you wish to store your data in a subdirectory, enter **`\backups\<subdirectory>\<filename>`** if the subdirectory exists before the command is sent. If any directory in the path does not exist, the command is denied because this command does not create directories.

4 Click **OK**.

You are asked to verify that you wish to backup to the directory that you entered. Click **Yes** if you typed the path correctly.

Result: The *Progress Indicator* screen appears, indicating that the backup is in progress. When the backup completes, a `Remote Backup successful` screen appears. Click **OK**. The backup file is now stored. If the default path and a subdirectory were used, the file can be found at:

```
C:\Program Files\Alcatel-Lucent\WaveStar CIT\backups\
<subdirectory>\<filename>
```

If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, the path could start with C:\Program Files\Lucent Technologies\.

END OF STEPS

Procedure 6-23.2: Restore NE database via FTAM

Overview

Use this procedure to restore the local NE database or a remote NE database (with OSI or DCC connectivity) via the File Transfer and Access Management (FTAM) protocol from the *WaveStar*® CIT.

Required equipment

Refer to "Required equipment" (p. 6-279) in Procedure 6-23: "Backup and restore NE database via FTAM" (p. 6-279) for a list of equipment required to perform this procedure.

Before you begin

Before performing this procedure, complete Procedure 6-23: "Backup and restore NE database via FTAM" (p. 6-279).

Steps

Complete the following steps to restore the local NE database.

1 **NOTICE**

Service-disruption hazard

Restoring the network element database can be service-affecting.

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

From the System View menu, select **Configuration** → **Software** → **Remote Restore**.

Important! If the TID has changed since the backup was performed, then the restore is denied. The software release of the backup database must be the same as the current software generic. In addition, if any service-related parameters (for example, cross-connections) have been changed since the last backup file was created, those changes are lost and service can be affected. These changes must be reentered.

2 In the pull-down **Restore From/Via:** menu, select **FTAM**.

3 In the **Source/Destination Directory Path** panel, enter the location where the database information is stored. Enter the path and filename exactly as it was entered in Procedure 6-23.1: “Backup NE database via FTAM” (p. 6-281). For example: `\backups\<subdirectory>\<filename>`.

You can also click the **Browse** button next to the *Path:* field to browse to any directory on your PC and select the required file.

> **Important!** The value of the Path field can be either an absolute path or a relative path that is relative to the FTP server root directory. The absolute path must start with the drive name followed by a colon (:) then the path names; for example: C:\temp\today\backup. The syntax of the relative path must start with the path name; for example: \temp\backup.
>
> The *WaveStar*® CIT directory automatically enters the relative path for the *WaveStar*® CIT. The default relative path is
>
> `C:\Program Files\Alcatel-Lucent\WaveStar CIT\`
>
> If you had an older *WaveStar*® CIT installed prior to installing the current *WaveStar*® CIT, the path could start with C:\Program Files\Lucent Technologies\.

4 Click **OK**.

You are asked to verify that you wish to restore from the directory that you entered. Click **Yes** if you typed the path correctly.

A second warning screen appears that states that Execution of RESTORE causes a System Reset. Click **Yes**.

> **Result:** The *Progress Indicator* screen appears, indicating that the restore is in progress. When the restore is complete, a *WaveStar*® CIT warning screen appears, stating *NE reset after successful restore, CIT is going to log out*.

5 Click **OK**.

> **Result:** A second *WaveStar*® CIT warning screen appears, stating *Communication to network element is lost, system view will now be closed.*

6 Click **OK**.

END OF STEPS

Procedure 6-24: Observe FTP progress

Overview

Use this procedure to observe the progress of a transfer via FTP.

Important! This procedure assumes that the *WaveStar*® CIT is your FTP Server and can only be performed if you selected **Enable WaveStar CIT FTP Server** during the *WaveStar*® CIT installation, refer to Procedure 6-1: "Install software on the PC" (p. 6-4). If you selected **Disable WaveStar CIT FTP Server**, you cannot use this procedure.

Required equipment

Only a personal Computer (PC) with *WaveStar*® CIT software (with **Enable WaveStar CIT FTP Server** selected) installed is required to perform this procedure.

Before you begin

Prior to performing this procedure, refer to "Before you begin" (p. 6-3) in this chapter.

Steps

Complete the observe FTP progress.

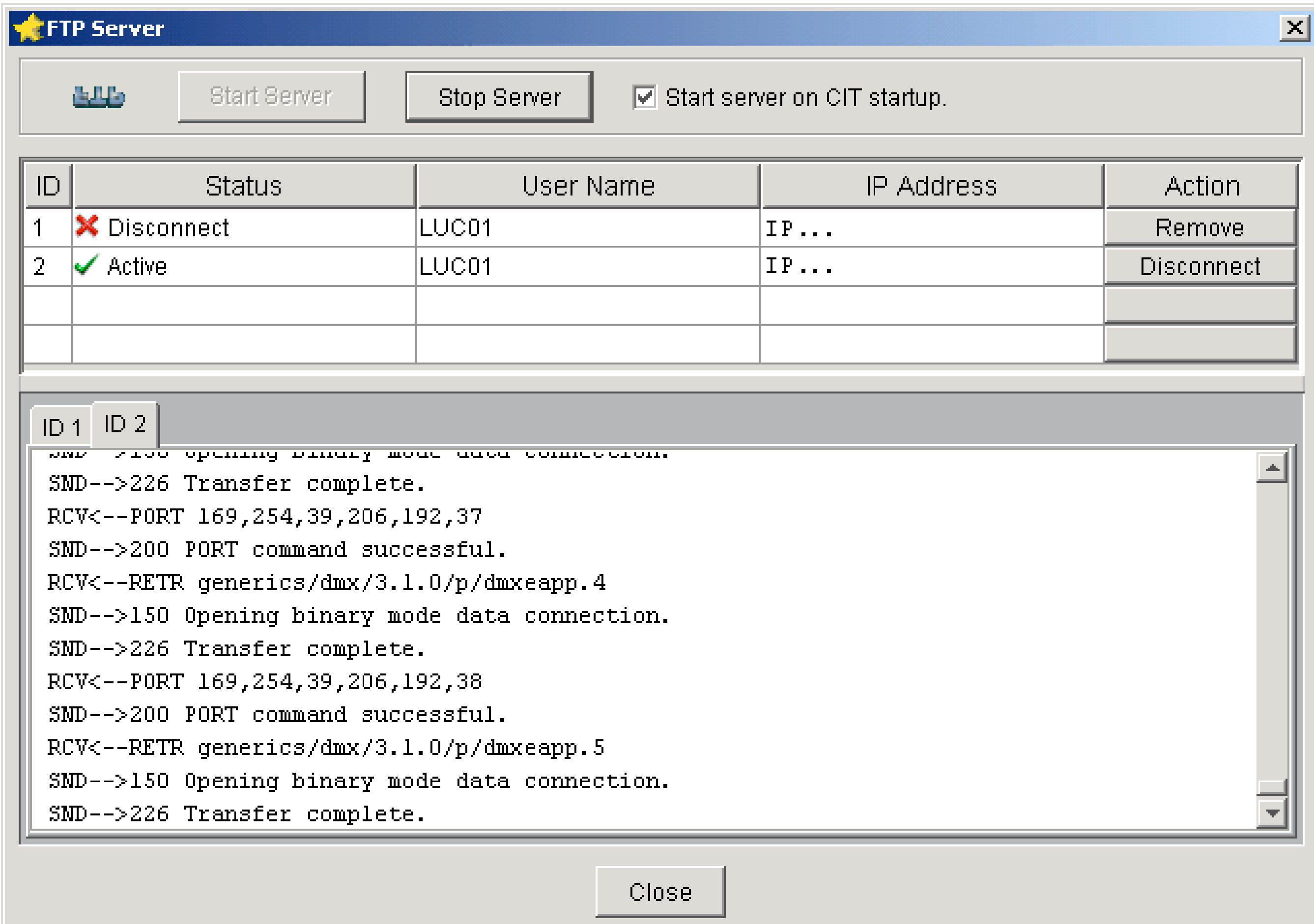
1 From the Network View, either

- select **Administration** → **FTP Administration**.

  or
- click on the rotating FTP icon in the lower left-hand corner of the Network View Window.

  Important! This step is executed from the Network View; most *WaveStar*® CIT activities are executed from the System View.

Result: The following FTP Server window opens.



The FTP server may display multiple FTP sessions listed by ID 1, 2.... The active session is identified by a green check-mark and the Status: Active. Older sessions are identified by a red X and the Status: Disconnect.

2 Identify the ID for the Active session and click on the corresponding IDx tab to view the transmission progress. When the transmission is complete, the Status for that ID changes to Disconnect. Click **Close** when finished.

Important! If the FTP server fails to start, it could mean that another program using an FTP server is already running. Depending on what operating system you are using, you must go to the device file and disable the FTP server. Refer to Procedure 6-25: "Disable an FTP server on your PC" (p. 6-287) for instructions for each allowed operating system.

END OF STEPS

Procedure 6-25: Disable an FTP server on your PC

Overview

Use this procedure to disable an FTP server application that is running on the personal computer being used for the *WaveStar*® CIT.

Required equipment

Only a personal Computer (PC) with *WaveStar*® CIT software installed is required to perform this procedure.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 6-3) in this chapter
2. Because multiple FTP applications might be installed on this PC, you must be able to identify the program you wish to disable.

Steps

Complete the following steps to disable an FTP server application.

1 Which Windows Operating System are you using?

If...	Then
Windows 2000	Continue with Step 2.
Windows XP	Proceed to Step 7.
Windows 7	Proceed to Step 11.

2 For Windows 2000 operating systems, select **Start** → **Settings** → **Control Panel**.

3 Select **Administrative Tools**, then **Computer Management**, then **Services and Applications**, and then **Services**.

4 Locate the FTP file that is running and double click the FTP icon.

5 In the **Service Status:** field, click **Stop**.

6 STOP! End of Procedure.

7 For Windows XP operating systems, select **Start** → **Control Panel**.

8 Click the **Performance and Maintenance** icon, then the **Administrative Tools** icon, and then **Services**.

9 Locate the FTP service that is running and select it.

10 Click **Stop**, then **Close**.

11 For Windows 7 operating systems, select **Start** → **Control Panel**.

12 Click the **Administrative Tools** icon and then **Services**.

13 Locate the FTP service that is running and select it.

14 Click **Stop**, then **Close**.

END OF STEPS

Procedure 6-26: Establish communications with Network Element

Steps

Complete the following steps to establish communications with the network element.

1 Using an RS-232 cable, connect an available COM port of the PC (9-pin D-type connector) to the **RS232** port on the faceplate of the SYSCTL circuit pack (RJ45-type connector).

2 Start a terminal emulation program (for example, TERM, Hyper Terminal) with the following settings:

- Baud Rate: 9600
- Character Size: 8
- Stop Bits:1
- Parity: none
- Flow Control: xon/xoff
- Local echo: off

3 When the program opens, connect to the COM port on the PC that is connected to the network element and press the **ENTER** key several times. Is the network element TID displayed?

If...	Then...
Yes,	Record the TID that was displayed and continue with the next step.
No,	Go to Step 5.

4 Using the TID that was displayed, attempt to log in to the network element. Was the log in attempt successful?

If...	Then...
Yes,	**STOP! End of Procedure.**
No,	Continue with the next step.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

5 Using a CAT5 cross-over Ethernet cable, connect the NIC card of the PC to the **LAN** port on the SYSCTL circuit pack faceplate. On the WaveStar CIT screen above the NE name on the left side, click on **View: TCP/IP Direct Connect** and change this to **CIT OSI Neighbors**. Is the network element TID displayed?

If...	Then...
Yes,	Continue with the next step.
No,	Go to Step 7.

6 Using the TID that was displayed, attempt to log in to the network element. Was the log in attempt successful?

If...	Then...
Yes,	**STOP! End of Procedure.**
No,	Continue with the next step.

Reference: Procedure 6-2: "Connect Personal Computer (PC) and establish *WaveStar*® CIT session" (p. 6-27)

7 Using a CAT5 cross-over Ethernet cable, connect the NIC card of the PC to the **J16 IAO LAN** port on the rear of the shelf.

8 Attempt to log in to the network element. Was the log in attempt successful?

If...	Then...
Yes,	**STOP! End of Procedure.**
No,	Continue with the next step.

Reference: Procedure 6-2: “Connect Personal Computer (PC) and establish *WaveStar*® CIT session” (p. 6-27)

9 Using a modem serial cable, connect the **J17 MODEM** port (RJ45-type connector) on the rear of the shelf through a null-modem connector to an available COM port of a PC.

10 Attempt to log in to the network element.

Reference: Procedure 6-2: “Connect Personal Computer (PC) and establish *WaveStar*® CIT session” (p. 6-27)

END OF STEPS

Procedure 6-27: Enter/exit pluggable transmission module maintenance state

Overview

Use this procedure to enter or exit the pluggable transmission module maintenance state.

Pluggable transmission module maintenance state

A pluggable transmission module enters the maintenance state when the pluggable transmission module Maintenance State parameter is provisioned to *Maint*.

When the Maintenance State parameter is provisioned to *Maint*, the system reports `Pluggable transmission module maintenance IP` and `ABN condition`. Any subsequent removal of the pluggable transmission module is reported with an alarm severity level no higher than a standing condition regardless of the assigned ASAP alarm severity level.

A pluggable transmission module remains in the maintenance state until the pluggable transmission module Maintenance State parameter is provisioned to *Normal* (default value). Any subsequent removal of the pluggable transmission module is reported using the applicable assigned ASAP alarm severity level.

Entering/exiting the Maintenance state does not affect the alarm severity level of any existing removal alarms.

Privilege level

You must log in as a Privileged or General user to complete this procedure.

Before you begin

Prior to performing this procedure:

1. Refer to "Before you begin" (p. 6-3) in this chapter.
2. Obtain the work instructions for this procedure.
3. Verify that the work instructions specify the required pluggable transmission module addresses.

Steps

Complete the following steps to enter or exit the pluggable transmission module maintenance state.

1 From the System View window, select **Configuration** → **Equipment**.

Result: The *Configure Equipment* window opens.

2 Find the circuit pack with the required pluggable transmission module, then expand the equipment list by clicking on the plus (+) sign next to the required circuit pack. Select the required *PTM* and click **Select**.

Result: The pluggable transmission module parameters appear.

3 **Important!** When the Maintenance State parameter is provisioned to *Maint*, the pluggable transmission module enters the maintenance state. When the Maintenance State parameter is provisioned to *Normal*, the pluggable transmission module exits the maintenance state.

Provision the *Maintenance State* parameter according to the work instructions, then click **Apply**. Click **Close** to exit.

END OF STEPS

Procedure 6-28: Replace DWDM optical multiplexer/demultiplexer circuit pack

Overview

Use this procedure to replace an LNW785 OMD5/8 circuit pack.

Before you begin

Prior to performing this procedure:

1. Refer to “Required equipment” (p. 6-3) in this chapter.
2. Refer to “Laser safety” (p. 1-6) and “Electrostatic discharge” (p. 1-26) information in Chapter 1, “Safety”.
3. Obtain work instructions for this procedure.
4. Ensure that the appropriate circuit pack is available for replacement.

Steps

Complete the following steps to replace an LNW785 OMD5/8 circuit pack.

1 If required, remove the cables from the circuit pack.

2 Remove the required circuit pack by grasping the inner edge of the locking-levers, and applying a constant pressure, pull the levers forward and remove the circuit pack.

3 Ensure that all optical fiber connectors and couplings are properly cleaned on the replacement circuit pack.

Important! Signal performance may be degraded if the connections and couplings are not cleaned properly.

Reference: Procedure 6-11: “Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)” (p. 6-151)

4 Seat the replacement circuit pack in vacated Function Unit slot.

Result: **FAULT** LED on the circuit pack lights. After approximately 60 seconds, the **ACTIVE** LED lights and the **FAULT** LED may go off. (Firmware updates may take place that add additional wait time.)

Select **View** → **Refresh System View** and the circuit pack appears in the *WaveStar*® CIT System View indicating successful installation.

If both the original circuit pack and the replacement circuit pack fail when no other transmission circuit packs are installed in the shelf, replace the SYSCTL circuit pack. Refer to Procedure 6-10: “Upgrade or replace SYSCTL (LNW2) circuit pack” (p. 6-99).

5 If required, reconnect the cables.

Result: The circuit pack **FAULT** LED stops flashing.

6 Ensure that a 177D apparatus blank or an LNW98 Detectable apparatus blank is present in the unequipped companion Function Unit slot.

7 From the System View menu, click the **Alarm List** button to obtain an *NE Alarm List*. Verify that no alarms are present for the installed circuit pack.

If required, refer to the appropriate procedure to clear any alarms.

8 From the System View menu, use **View** → **Equipment** to access the circuit pack/port parameters for the circuit pack just installed and verify that the parameters are intact.

If required, refer to the appropriate procedure in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* to change any circuit pack/port parameters.

END OF STEPS

Procedure 6-29: Replace 10G Muxponder circuit pack

Overview

Use this procedure to replace an LNW705 XM10G/8 10G Muxponder circuit pack.

Required equipment

Use only Alcatel-Lucent Approved Class 1 XFP and SFP transceivers. Refer to the list of pluggable transmission modules in Procedure 6-8: "Replace pluggable transmission module" (p. 6-71).

Refer to the *Alcatel-Lucent 1665 Data Multiplexer (DMX) Installation Manual, 365-372-304*, as required, when removing and/or installing pluggable transmission modules.

Before you begin

Prior to performing this procedure:

1. Refer to "Required equipment" (p. 6-3) in this chapter.
2. Refer to "Laser safety" (p. 1-6) and "Electrostatic discharge" (p. 1-26) information in Chapter 1, "Safety".
3. Obtain work instructions for this procedure.
4. Ensure that the appropriate circuit pack/pluggable transmission modules are available for replacement.

Steps

Complete the following steps to replace an XM10G/8 circuit pack.

1 Remove the cables from the circuit pack.

2 Remove the pluggable transmission modules from the circuit pack.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

3 Remove the required circuit pack by grasping the inner edge of the locking-levers, and applying a constant pressure, pull the levers forward and remove the circuit pack.

4 Ensure that all optical fiber connectors and couplings are properly cleaned on the replacement circuit pack.

Important! Signal performance may be degraded if the connections and couplings are not cleaned properly.

Reference: Procedure 6-11: "Clean optical fibers, dual LC adapters and LC lightguide buildouts (LBOs)" (p. 6-151)

5 **Important!** Pluggable transmission modules are shipped with a dust cover installed into the optical ports to maintain cleanliness during storage and/or transportation. It is recommended that the dust cover be kept in place to maintain cleanliness until the optical fiber is connected. With proper care and handling, cleaning the pluggable transmission modules should not be necessary.

Clean the optical pluggable transmission modules.

Reference: Procedure 6-12: "Clean optical pluggable transmission module" (p. 6-160)

6 Seat the replacement circuit pack in vacated Function Unit slot.

Result: **FAULT** LED on the circuit pack lights. After approximately 60 seconds, the **ACTIVE** LED lights and the **FAULT** LED may go off. (Firmware updates may take place that add additional wait time.)

Select **View** → **Refresh System View** and the circuit pack appears in the *WaveStar*® CIT System View indicating successful installation.

If both the original circuit pack and the replacement circuit pack fail when no other transmission circuit packs are installed in the shelf, replace the SYSCTL circuit pack. Refer to Procedure 6-10: "Upgrade or replace SYSCTL (LNW2) circuit pack" (p. 6-99).

7 Install the pluggable transmission modules.

Reference: Procedure 6-8: "Replace pluggable transmission module" (p. 6-71)

8 Reconnect the cables.

Result: The circuit pack **FAULT** LED or port LED associated with the pluggable transmission module stops flashing.

9 Ensure that a 177D apparatus blank or an LNW98 Detectable apparatus blank is present in the unequipped companion Function Unit slot.

10 From the System View menu, click the **Alarm List** button to obtain an *NE Alarm List*. Verify that no alarms are present for the installed circuit pack.

If required, refer to the appropriate procedure to clear any alarms.

11 From the System View menu, use **View** → **Equipment** to access the circuit pack/port parameters for the circuit pack just installed and verify that the parameters are intact.

If required, refer to the appropriate procedure in the *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301* to change any circuit pack/port parameters.

END OF STEPS

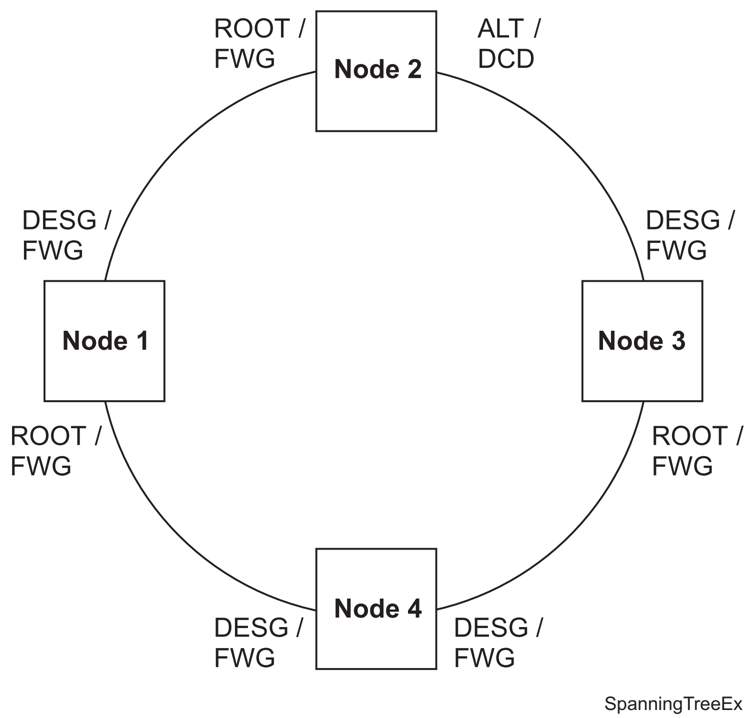
Procedure 6-30: Verify spanning tree configuration

Overview

Use this procedure to verify the spanning tree configuration.

Spanning tree network example

The following figure shows an example of a simple spanning tree network in a ring configuration with the spanning tree role and spanning tree status of each participating port.



The spanning tree role values are:

- ROOT - Port is used for transmission and is the best path to the root node
- DESG (Designated) - Port is used for transmission; however, the port is not the best path to the root node
- ALT (Alternate) - Port is not used for transmission

The spanning tree status values are:

- FWG: Forwarding
- BLK: Blocked - 802.1D mode only
- LLG: Learning/Listening

- DISA: Disabled - Administration
- DISF: Disabled - Failure
- DCD: Discarding - 802.1w mode only

In this example, Node 4 is elected the *root node* by the spanning tree protocol. The root node can be identified by observing the spanning tree role of the participating ports. At the root node, all the participating ports have a spanning tree role of either DESG (designated) or ALT (alternate). The participating ports at the root node do *not* have a spanning tree role of ROOT.

Because there is a transmission loop in the example spanning tree network, the spanning tree role of a port at Node 2 is ALT (alternate) and the port is not used for transmission.

The spanning tree role of the remaining participating ports in the example is DESG (designated).

In this example, all ports have a FWG (forwarding) spanning tree status, except for the ALT port at Node 2. The ALT port has a DCD (discarding) or BLK (blocked) spanning tree status.

Procedure

Complete the following steps to verify the spanning tree configuration.

1 Using office records and the work instructions determine the affected Ethernet spanning tree networks to be verified. Make a sketch of each spanning tree network with all participating nodes/ports using Rapid Spanning Tree Protocol and their connectivity.

Reference: Refer to the example in "Spanning tree network example" (p. 6-299).

2 Identify a spanning tree network to be verified.

3 At each node in the spanning tree network, select **View** → **Data** → **Spanning Tree Group** to access the required spanning tree group and record the required *Port Role* and *Status* parameter values for the participating ports.

4 **Important!** There must be exactly one root node in the spanning tree network. At the root node, all the participating ports have a *Port Role* of either DESG (designated) or ALT (alternate). None have ROOT.

Using the information obtained in the previous step, determine the root node by observing the *Port Role* of the participating ports at each node.

5 For all nodes except the root node, verify that each node has one participating port with a *Port Role* of ROOT.

6 Verify the appropriate forwarding status of the remaining ports.

If...	Then...
a ring network	verify that exactly one port has a *Port Role* of ALT with a *Status* of DCD or BLK. No port should have a *Status* of DISF or DISA.
a mesh network where there may be multiple redundant paths (loops),	verify that there are exactly enough ports with a *Port Role* of ALT and a *Status* of DCD or BLK to break all loops but still allow a path from every other node to the root node. No port should have a *Status* of DISF or DISA.

7 If required, change the existing spanning tree configuration.

If any port has a *Status* of DISF or DISA, clear all Ethernet-related alarms/conditions and/or verify provisioning using office records.

Reference: *Alcatel-Lucent 1665 Data Multiplexer (DMX) User Operations Guide, 365-372-301*

If required, contact Technical Support Services (TSS) for assistance in changing the spanning tree configuration.

END OF STEPS

Glossary

Type of diagnostic test used to compare an original transmitted signal with the resulting received signal. A loopback is established when the received optical or electrical external transmission signal is sent from a port or tributary input directly back toward the output.

Symbols

µ

Microns

µm

Micrometer

Numerics

1+1 (bidirectional)

The bidirectional 1+1 protection switching architecture protects against failures of the optical transmit/receive equipment and their connecting fiber facility. One bidirectional interface (two fibers plus associated OLIUs on each end) is designated "service," and the other is designated "protection." In each direction, identical signals are transmitted on the service and protection lines ("dual-fed"). The receiving equipment monitors the incoming service and protection lines independently and selects traffic from one line (the "active" line) based on performance criteria and technician/OS control. In bidirectional 1+1 switching, the network elements are not independent. When a protection switch is requested at a network element, both network elements perform protection switching.

1+1 (unidirectional)

The unidirectional 1+1 protection switching architecture protects against failures of the optical transmit/receive equipment and their connecting fiber facility. One bidirectional interface (two fibers plus associated OLIUs on each end) is designated "service," and the other is designated "protection." In each direction, identical signals are transmitted on the service and protection lines ("dual-fed"). The receiving equipment monitors the incoming service and protection lines independently and selects traffic from one line (the "active" line) based on performance criteria and technician/OS control. In unidirectional 1+1 switching, both service and protection lines could be active at the same time (service in one direction, protection in the other).

1GE

Gigabit Ethernet - 1.250 Gbps line rate.

1xN, 1x1

1xN protection switching pertains to circuit pack protection that provides a redundant signal path through Alcatel-Lucent 1665 DMX (it does not cover protection switching of an optical facility; see "1+1"). In 1xN switching, a group of N service circuit packs share a single spare protection circuit pack. 1x1 is a special case of 1xN, with N=1. In 1x1, only one is active at a time.

802.1Q Mode

In 802.1Q Mode, a circuit pack can be provisioned to use an incoming frame's VLAN tag either to add a VLAN tag associated with the port for untagged frames or to drop an incoming frame if its VLAN tagging does not meet provisioned specifications. The priority bits in an incoming frame's VLAN tag can also be used to affect the handling of the frame.

A

ABN

Abnormal (status condition)

AC

Alternating Current

ACIDs

Application Context IDs

Active

Active identifies any protected entity which is currently selected by the receiver at either end as the payload carrying signal that is currently carrying service (see Standby).

Adaptive Rate

See Pipe Mode.

Add/Drop Multiplexer (ADM)

The term for a synchronous network element capable of combining signals of different rates and having those signals added to or dropped from the stream.

ADM

Add/drop multiplexer

ADR

Add/drop ring

Aging

The filtering database entries are automatically removed after an aging period (300 seconds).

AGNE

Alarm gateway network element

AIS

Alarm indication signal

Alarm

Visible or audible signal indicating that an equipment failure or significant event/condition has occurred.

Alarm Cut-Off (ACO)

A button on the SYSCTL used to silence audible alarms.

Alarm Gateway Network Element (AGNE)

A defined network element in an alarm group through which members of the alarm group exchange information.

Alarm Indication Signal (AIS)

A code transmitted downstream in a digital network that shows that an upstream failure has been detected and alarmed.

Alarm Severity Assignment Profile (ASAP)

A user provisioned mechanism to control an alarm level.

Alien Wavelength

A compatible DWDM optical signal that is sourced or terminated by a different network element.

Alternate Mark Inversion (AMI)

A line code that employs a ternary signal to convey binary digits, in which successive binary ones are represented by signal elements that are normally of alternating, positive and negative, polarity but equal in amplitude, and in which binary zeros are represented by signal elements that have zero amplitude.

American Standard Code for Information Interchange (ASCII)

A standard 7-bit code that represents letters, numbers, punctuation marks, and special characters in the interchange of data among computing and communications equipment.

AMI

Alternate Mark Inversion

ANSI

American National Standards Institute

APD

Avalanche PhotoDiode

APS

Automatic Protection Switch

APS Channel

The signalling channel carried in the K1 and K2 bytes of the SONET overhead on the protection line. It is used to exchange requests and acknowledgments for protection switch actions.

ASAP

Alarm Severity Assignment Profile

ASCII

American Standard Code for Information Interchange

ASN.1

Abstract Syntax Notation 1

Asynchronous Transfer Mode (ATM)

A high-speed transmission technology characterized by high bandwidth and low delay. It utilizes a packet switching and multiplexing technique which allocates bandwidth on demand.

ATM

Asynchronous Transfer Mode

Auto

Automatic

Auto

One possible state of ports, lines, and channels. In this state, the port, line, or channel will automatically be put "in service" if a good signal is detected coming from the DSX panel.

Automatic Protection Switch

A feature that allows another source to be automatically selected and reconfigured in the event of a source failure or network change; for example, a fiber cut.

Avalanche Photodiode (APD)

A diode that increases its electrical conductivity by a multiplication effect when hit by light. APDs are used in lightwave receivers because the APDs have a greater sensitivity to weakened light signals (for example, those which have traveled long distances over fiber).

B

B3ZS

Bipolar 3-Zero Substitution

B8ZS

Bipolar 8-Zero Substitution

Backbone Ring

A host ring.

Backout

Refers to backing out of an upgrade in progress. A backout returns a node(s) to the pre-upgrade state.

Backup

The backup and restoration features provide the capability to recover from loss of network element data because of such factors as human error, power failure, and network element design flaws.

Bandwidth

The difference in Hz between the highest and lowest frequencies in a transmission channel. The data rate that can be carried by a given communications circuit.

Baud Rate

Transmission rate of data (bits per second) on a network link.

BDFB

Battery Distribution and Fuse Bay

BER

Bit Error Rate

Bidirectional Line

A transmission path consisting of two fibers that handle traffic in both the transmit and receive directions.

Bidirectional Line-Switched Ring (BLSR)

A bidirectional ring in which protection switching is accomplished by switching working traffic into protection time slots in the line going in the opposite direction around the ring.

Bidirectional Ring

A ring in which both directions of traffic between any two nodes travel through the same network elements (although in opposite directions).

Bidirectional Switch

Protection switching performed in both the transmit and receive directions.

BIP

Bit Interleaved Parity

Bipolar 8-Zero Substitution (B8ZS)

A line coding technique that replaces eight consecutive zeros with a bit sequence having special characteristics accomplishing two objectives: First, this bit sequence accommodates the density requirements of the ones for digital T1 carrier; second, the sequence is recognizable at the destination (due to deliberate bipolar violations) and is removed to produce the original signal.

Bit

The smallest unit of information in a computer, with a value of either 0 or 1.

Bit Error Rate (BER)

The ratio of error bits received to the total number of bits transmitted.

Bit Error Rate Threshold

The point at which an alarm is issued for bit errors.

Bit Interleaved Parity-N(BIP-N)

A method of error monitoring over a specified number of bits (BIP-3 or BIP-8).

BITS

Building Integrated Timing Supply

BITS clock

A BITS (Building Integrated Timing Source) clock is a clock within a central office that distributes timing to all the equipment in that central office. The BITS clock is tied to an external, stable timing source, such as a GPS (global positioning satellite).

Blocking

The state in which an Ethernet port does not participate in frame relay. The forwarding process discards received frames.

BLSR

Bidirectional line-switched ring

BPDU

Bridge protocol data unit

Bridge Cross-Connection

Setting up a cross-connection leg with the same input tributary as that of an existing cross-connection leg, forming a 1:2 bridge from an input tributary to two output tributaries.

Broadband

Any communications channel with greater bandwidth than a voice channel; sometimes used synonomously with wideband.

Burst Size

The provisioned burst size determines the length or size of the data burst that is allowed by the peak information rate policer. This affects policing for all VLANs (in 802.1Q mode), all port tags (in transparent mode), and all Private Line services (in Private Line or No Tag mode) on the LNW66 Ethernet circuit packs.

Byte

Refers to a group of eight consecutive binary digits.

C

C-Bit

A framing format used for DS3 signals produced by multiplexing 28 DS1s into a DS3. This format provides for enhanced performance monitoring of both near-end and far-end entities.

CC

Clear Channel

CCITT

Comité Consultatif International Télégrafique & Téléphonique
(International Telephone and Telegraph Consultative Committee)

CCITT - International Telephone and Telegraph Consultative Committee

An international advisory committee under United Nations sponsorship that has composed and recommended for adoption worldwide standards for international communications. Recently changed to the International Telecommunications Union Telecommunications Standards Sector (ITU-TSS).

CD-ROM

Compact Disk, Read-Only Memory

Channel

A logical signal within a port. For example, for an EC-1 port, there is one STS-1 channel and sometimes 28 VT1.5 channels. See Port.

Channel State Provisioning

A feature that allows a user to suppress reporting of alarms and events during provisioning by supporting multiple states (automatic, in-service and not monitored) for VT1.5 and STS-n channels. See Port State Provisioning.

Circuit

A set of transmission channels through one or more network elements that provides transmission of signals between two points to support a single communications path.

CIT

Craft Interface Terminal

Clear Channel (CC)

A provisionable mode for the DS3 output that causes parity violations not to be monitored or corrected before the DS3 signal is encoded.

CLEI

Common Language Equipment Identifier

Client Signal Fail (CSF)

The local network element sends a Client Signal Fail (CSF) signal to the far-end equipment when a defect is detected in the ingress client signal (Ethernet/Data protocol).

CLK

Clock

CMISE

Common Management Information Service Element

CO

Central Office

Coding Violation (CV)

A performance monitoring parameter indicating that bipolar violations of the signal have occurred.

Collocated

System elements that are located in the same location.

Concatenation

A procedure whereby multiple virtual containers are associated with each other resulting in a combined capacity that can be used as a single container across which bit sequence integrity is maintained.

Constituent Signals

List of received signals for an adaptive rate (pipe mode) optical port.

Cost

Cost is used to help determine the efficiency of any given path. Cost is provisioned for a port (depending on speed of transmission) and calculated automatically for a path (sum of the port costs for the path).

CP

Circuit Pack

CPE

Customer Premises Equipment

CR

Critical (alarm status)

Craft Interface Terminal (CIT)

The user interface terminal used by craft personnel to communicate with a network element.

Credit Interval

The provisioned interval for adding tokens to the token bucket used by the peak information rate policer. This affects policing for all VLANs (in 802.1Q mode), all port tags (in transparent mode), and all Private line services (in Private Line or No Tag mode).

Critical (CR)

Alarm that indicates a severe, service-affecting condition.

CRN

Customer Release Notes

Cross-Connect Capacity

The total bandwidth of cross-connections as measured by the bandwidth of input and output tributaries. A system with N STS-1 equivalent input tributaries and N STS-1 equivalent output tributaries (referred to as "NxN") provides a cross-connection capacity of N STS-1 equivalents. This system could provide N one-way point-to-point cross-connections or N^2 two-way point-to-point cross-connections at the equivalent rate of STS-1.

Cross-Connect Loopback

A cross-connection from an input tributary to the output of that same tributary via the cross-connect fabric.

Cross-Connect Rate

The attribute of a cross-connection that defines the constituent signal rate(s) it can carry. For a cross-connection with an STS-3 "pipe" cross-connection rate, the constituent signals carried by the cross-connection can be either an STS-3c signal or three STS-1 signals. Similarly, for a cross-connection with an STS-12 "pipe" cross-connection rate, the constituent signals carried by the cross-connection can be either an STS-1 signal or an allowed mix of STS-12c signals and STS-3c signals.

CSF

Client Signal Fail

CTL

Controller

CTS

Customer Technical Support; now known as Technical Support Services (TSS)

Cut-Through

Refers to a simple ASCII interface to an network element. It enables the user to send TL1 messages directly to the network element with no interpretation or assistance provided by the WaveStar CIT.

CV

Coding Violation

CVFE

Coding Violation Far End

D

DACS

Digital Access Cross-Connect System

DACS III-2000

Digital Access and Cross-Connect System that provides clear channel switching at either the DS3 or the STS-1 rates, eliminating the need for manual DSXs.

DACS IV-2000

Digital Access and Cross-Connect System that provides electronic DS3/STS-1 or DS1/VT1.5 cross-connect capability, eliminating the need for manual DSXs.

Data Communications Channel (DCC)

The embedded overhead communications channel in the synchronous line, used for end-to-end communications and maintenance. The DCC carries alarm, control, and status information between network elements in a synchronous network.

Data Communications Equipment (DCE)

The equipment that provides signal conversion and coding between the data terminating equipment (DTE) and the line. The DCE may be separate equipment or an integral part of the DTE or of intermediate equipment. A DCE may perform other functions usually performed at the network end of the line.

Data Terminating Equipment (DTE)

The equipment that originates data for transmission and accepts transmitted data.

dB

Decibels

DC

Direct Current

DCC

Data Communications Channel

DCE

Data Communications Equipment

DDM-2000

Alcatel-Lucent SONET multiplexers that multiplex DS1, DS3, or EC-1 inputs into EC-1, OC-1, OC-3, or OC-12 outputs.

Default Provisioning

The parameter values that are preprogrammed as shipped from the factory.

Demultiplexing

A process applied to a multiplexed signal for recovering signals combined within it and for restoring the distinct individual channels of these signals.

DEMUX

Demultiplexer

DEMUX - Demultiplexer

The DEMUX direction is from the fiber toward the DSX.

Dense Wavelength Division Multiplexing (DWDM)

Transmitting two or more signals of different wavelengths simultaneously over a single fiber.

Digital Cross-Connect Panel (DSX)
A panel designed to interconnect to equipment that operates at a designated rate. For example, a DSX-3 interconnects equipment operating at the DS3 rate.

Digital Multiplexer
Equipment that combines time-division multiplexing several digital signals into a single composite digital signal.

Digital Signal Levels 0, 1, 3 (DS0, DS1, DS3)
An ANSI-defined signal or service level corresponding to the following: DS0 is 64 Kb/s, DS1 is 1.544 Mb/s (equivalent to T1), and DS3 is 44.736 Mb/s (equivalent to 28 T1 channels or T3).

Directory Services Network Element (DSNE)
A designated network element that is responsible for administering a database that maps network element names (TIDs) to addresses (NSAPs - network service access points) in an OSI subnetwork. There can be one DSNE per ring. Can also be a GNE.

Disable admin
An Ethernet port that does not participate in the spanning tree. The port is disabled by management.

Disable failure
A port in this state does not participate in the spanning tree. The port is disabled due to a hardware or software failure.

DLC
Digital Loop Carrier

DRI
Dual Ring Interworking

DS1
Digital Signal Level 1

DS3
Digital Signal Level 3

DS3 Format
Specifies the line format of a DS3 interface port, such as M23 or C-bit parity.

DSCP
Differentiated Services Code Point

DSLAM
Digital Subscriber Line Access Multiplexer

DSNE
Directory Services Network Element

DSX

Digital Cross-Connect Panel

DTE

Data Terminating Equipment

Dual Homing

A network topology in which two OC-3, OC-12, or OC-48 shelves serve as hosts.

DWDM

Dense Wavelength Division Multiplexing

E

E1

E1 is an SDH/PDH (Synchronous Digital Hierarchy/Pleiseosynchronous Digital Hierarchy, the European equivalent of SONET/DSx) electrical signal comparable to (but slightly faster than) a DS1. E1 is also sometimes called CEPT-1 (Conference of European Posts and Telecommunications) and is at 2.048 Mb/s.

EC-1

Electrical Carrier Level 1

EC-1, EC-n - Electrical Carrier

The basic logical building block signal with a rate of 51.840 Mb/s for an EC-1 signal and a rate of n times 51.840 Mb/s for an EC-n signal. An EC-1 signal can be built in two ways: A DS1 can be mapped into a VT1.5 signal and 28 VT1.5 signals multiplexed into an EC-1 (VT1.5 based EC-1), or a DS3 can be mapped directly into an EC-1 (DS3 based EC-1).

ECI

Equipment Catalog Item

EEPROM

Electrically-Erasable Programmable Read-Only Memory

EIA

Electronic Industries Association

Electromagnetic Compatibility (EMC)

A measure of equipment tolerance to external electromagnetic fields.

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)
Static electrical energy potentially harmful to circuit packs and humans.

EMC
Electromagnetic Compatibility

EMI
Electromagnetic Interference

Enterprise Systems Connection (ESCON)
A 200-Mb/s data signal used in storage area networking applications.

EOOF
Excessive Out of Frame

EoS
Ethernet over SONET

EPORT
Ethernet Port

EPROM
Erasable Programmable Read-Only Memory

EQ
Equipped (memory administrative state)

EQPT
Equipment

Equipment Catalog Item (ECI)
The bar code number on the faceplate of each circuit pack used by some inventory systems.

Errored Seconds (ES)
A performance monitoring parameter.

ES
Errored Seconds

ESD
Electrostatic Discharge

ESF
Extended Super Frame

EST
Environmental Stress Testing

Establish

A user-initiated command, at the WaveStar CIT, to create an entity and its associated attributes in the absence of certain hardware. (Does not apply to Alcatel-Lucent 1665 DMX

Event

A significant change. Events in controlled network elements include signal failures, equipment failures, signals exceeding thresholds, and protection switch activity. When an event occurs in a controlled network element, the controlled network element will generate an alarm or status message and send it to the management system.

Extended Superframe Format (ESF)

A T1 format that uses the framing bit for non-intrusive signaling and control. A T1 frame is sent 8,000 times a second, with each frame consisting of a payload of 192 bits, and with each frame preceeded by a framing bit. Because ESF only requires 2,000 framing bits for synchonization, the remaining 6,000 framing bits can be used for error detection.

Externally Timed

An operating condition of a clock in which it is locked to an external reference and is using time constants that are altered to quickly bring the local oscillator's frequency into approximate agreement with the synchronization reference frequency.

Extra traffic

Unprotected traffic that is carried over protection channels when their capacity is not used for the protection of working traffic. However, the extra traffic is unprotected and is preempted (lost) if a protection switch is activated. Preempted traffic is reestablished when the protection switch clears.

F

Facility

A one- or two-way circuit that carries a transmission signal.

Facility Loopback

A facility loopback is where an entire line is looped back.

Facility Roll

The disconnection of the circuit cross-connecting input tributary to an output tributary followed, within the required completion time, by a cross-connection of an input tributary to an output tributary.

Failure Rate (FIT)

Circuit pack failure rates per 10^9 hours as calculated using the method described in Reliability Prediction Procedure for Electronic Equipment, *Telcordia* ® Method I, Issue 5, September 1995. One FIT represents one failure per billion operating hours.

Far End (FE)

Any other network element in a maintenance subnetwork other than the one the user is at or is working on. Also called remote.

Far-End Receive Failure (FERF)

An indication returned to a transmitting network element that the receiving network element has detected an incoming section failure. Also known as RFI (Remote Failure Indication).

Fault

Term used when a circuit pack has a hard (not temporary) fault and cannot perform its normal function.

Fault Management

Collecting, processing, and forwarding of autonomous messages from network elements.

FC

Fibre Channel

FC - 1G

Fibre Channel - 1 Gigabit

FC -2G

Fibre Channel - 2 Gigabit

FC-100

Fibre Channel 100 MBps Interface - 1.0625 Gbps line rate.

FC-200

FFibre Channel 200 MBps Interface - 2.125 Gbps line rate.

FCC

Federal Communications Commission

FE

Far End

FE

Fast Ethernet

FE ACTY

Far End Activity

FEBE

Far End Block Error

FEC

Forward Error Correction

FEPROM

Flash EPROM

Fibre Channel - 1G (FC-1G)

A Fibre Channel 1.0625 Gb/s data signal.

Fibre Channel -2G (FC-2G)

A Fibre Channel 2.1250 Gb/s data signal.

Fibre Connection (FICON)

A 1.0625 Gb/s data signal.

File Transfer and Access Management (FTAM)

FTAM is the Open Systems Interconnection (OSI) standard for file transfer, file access, and file management.

Filtering database

The filtering database maintains a dynamic list of paths to which packets should be routed based on the destination address. The database entries are created, updated, and removed by the learning process.

FIT

Failures in 10^9 hours of operation.

Flash EPROM

A technology that combines the nonvolatility of EPROM with the in-circuit reprogrammability of EEPROM (electrically-erasable PROM).

FN

Function Unit

Forced

Term used when a protected entity (either working or protection) has been locked into a service-providing state by user command.

Forced Switch to Protection

The WaveStar CIT command that forces the protection group to be the "Active Unit." The clear command is required to remove the Forced Switch state. While in the Forced Switch state, the system may not switch the active unit either automatically, by means of the WaveStar CIT Forced Switch or Manual Switch command.

Forwarding

The state in which an Ethernet port participates in frame relay.

Free Running

An operating condition of a clock in which its local oscillator is locked to an internal synchronization reference and is using no storage techniques to sustain its accuracy.

FT-2000

An Alcatel-Lucent SONET OC-48 Lightwave System.

FTAM

File Transfer and Access Management

FTAM-FTP Gateway

The Alcatel-Lucent 1665 DMX supports an FTAM-FTP gateway function. This is also referred to as file transfer translation device (FTTD). The FTTD translates FTAM over OSI presentation to FTP over TCP/IP.

FTP

File Transfer Protocol

FTTD

File Transfer Translation Device

Function Unit (FN)

Refers to any one of a number of different circuit packs that can reside in the A, B, C, or D function unit slots on Alcatel-Lucent 1665 DMX.

G

Gateway Network Element (GNE)

A network element that passes information between other network elements and management systems through a data communication network.

GB

Gigabytes

Gb/s

Gigabits per second

GbE

Gigabit Ethernet

Generic Framing Procedure (GFP)

The Generic Framing Procedure, described in ITU-T G.7041/Y1303, provides a generic mechanism to adapt traffic from higher-layer client signals over a SONET network.

GFP

Generic Framing Procedure

GHz

Gigahertz

GNE

Gateway Network Element

GR-XXX

Telcordia ® General Requirement-XXX

GUI

Graphical User Interface

H **Hairpin Routing**

A cross-connection between function units (inter-function unit). For example, function unit C to function units A, B, or D. Also, a cross-connection within the same function unit (intra-function unit). Cross-connections go through Main, but no bandwidth or time slots are taken from the backbone ring. Eliminates need for another shelf.

Hashed FTP

The hashed FTP (digital signature) capability prevents tampering with a downloadable software image.

Holdover

An operating condition of a network element in which its local oscillator is not locked to any synchronization reference but is using storage techniques to maintain its accuracy with respect to the last known frequency comparison with a synchronization reference.

HS

High Speed

Hz

Hertz

I **I/O**

Input/Output

IAO LAN

Intraoffice Local Area Network

ID

Identifier

IEC

International Electrotechnical Commission

IEEE

Institute of Electrical and Electronics Engineers

IMF

Infant Mortality Factor

In-Service (IS)

A memory administrative state for ports. IS refers to a port that is fully monitored and alarmed.

INC

Incoming Status

Insert

To physically insert a circuit pack into a slot, thus causing a system-initiated restoral of an entity into service and/or creation of an entity and associated attributes.

Intermediate Reach (IR)

A term used to describe distances of 15 to 40 km between optical transmitter and receiver without regeneration. See long reach.

IP

Internet Protocol

IR

Intermediate Reach

IS

In Service

ISDN

Integrated Services Digital Network

ISO

International Standards Organization

ISP

Internet Service Provider

J

Jitter

Timing jitter is defined as short-term variations of the significant instants of a digital signal from their ideal positions in time.

Jumbo frame

Jumbo frames increase network efficiency by reducing the number of frames to be processed.

K

Kb/s

Kilobits per second

L

LAG

Link Aggregation Group

LAN

Local Area Network

LAPD

Link Access Procedure "D"

LBC

Laser Bias Current

LBO

Lightguide Build Out

LCAS

Link Capacity Adjustment Scheme

LCN

Local Communications Network

LEC

Local Exchange Carrier

LED

Light-Emitting Diode

LFD

Loss of Frame Delineation

LGX

Lightguide Cross-Connect

Light Emitting Diode (LED)

Used on a circuit pack faceplate to show failure (red) or service state. It is also used to show the alarm and status condition of the system.

Lightguide Build-Out (LBO)

An attenuating (signal-reducing) element used to keep an optical output signal strength within desired limits.

Lightguide Cross-Connect (LGX)

A SONET device that contains ports for optical fiber connections to an optical network element. An LGX is used to make and change connections to an network element without changing the cabling on the network element itself.

Line

A transmission medium, together with the associated equipment, required to provide the means of transporting information between two consecutive network elements. One network element originates the line signal; the other terminates it.

Line Timing

The capability to directly derive clock timing from an incoming OC-N signal while providing the user the capability to provision whether switching to an alternate OC-N from a different source (as opposed to entering holdover) will occur if the OC-N currently used as the timing reference for that network element becomes unsuitable as a reference. For example, intermediate nodes in a linear network are line timed. See Loop Timing.

Link Aggregation

A method of combining a group of IEEE 802.3 Ethernet links into a single logical link of up to the aggregate rate.

Link Capacity Adjustment Scheme (LCAS)

LCAS is an enhancement to SONET/SDH Virtual Concatenation that allows adding or removing Virtual Concatenation Group (VCG) members, to vary its bandwidth, by management command. It also automatically removes and restores failed members.

Listening

The state in which an Ethernet port is preparing to participate in frame relay. In the listening state, frame relay is disabled. This is an interim state between blocking and learning.

LOA

Loss of Alignment

Local

See Near-End.

Local Area Network (LAN)

A communications network that covers a limited geographic area, is privately owned and user administered, is mostly used for internal transfer of information within a business, is normally contained within a single building or adjacent group of buildings, and transmits data at a very rapid speed.

Locked DSn Cross-Connections

Locked DSn cross-connections add/drop traffic to/from only one rotation of a UPSR. Path switching is disabled. Time slots can be reused at different nodes around the UPSR.

LOF

Loss of Frame

Long Reach (LR)

A term used to describe distances of 40 km or more between optical transmitter and receiver without regeneration. See Intermediate Reach.

LOP

Loss of Pointer

LOS

Loss of Signal

Loss of Alignment (LOA)

One or more STS-1s that compose a VCG are out of multiframe alignment because of excess delay difference.

Loss of Frame (LOF)

A failure to synchronize to an incoming signal.

Loss of Frame Delineation (LFD)
Lack of sufficient bandwidth that is reported when there is a mismatch in the number of STS tributaries.

Loss of Pointer (LOP)
A failure to extract good data from an STS-n payload.

Loss of Signal (LOS)
The complete absence of an incoming signal.

LPBK
Loopback

LR
Long Reach

LS
Low Speed

M

M23-Format
A standard framing format used for DS3 signals produced by multiplexing 28 DS1s into a DS3 (sometimes referred to as M13-format, without C-bit parity).

MAC
Media Access Control

MAC Address
A unique hardware address that identifies each node of a network.

Main
The two slots (M1 and M2) on an Alcatel-Lucent 1665 DMX shelf in which the OC-n (n = 3, 12, 48, or 192) high-speed OLIU circuit packs are installed.

Main shelf
A shelf in a multi-shelf configuration that has one or more provisioned sub-tending sub-shelves.

Maintenance Condition
An equipment state in which some normal service functions are suspended, either because of a problem or to perform special functions (copy memory) that cannot be performed while normal service is being provided.

Major
Indicates a service-affecting failure, main or unit controller failure, or power supply failure.

MB
Megabytes

Mb/s
Megabits per second

Minor (MN)
Indicates a nonservice-affecting failure of equipment or facility.

Miscellaneous Discrete Interface
Allows an operations system to control and monitor equipment collocated within a set of input and output contact closures.

MJ
Major Alarm

MM
Multimode

MML
huMan-Machine Language

MN
Minor Alarm

MPEG
Moving Picture Experts Group

MSPP
Multi Service Provisioning Platform

MTBF
Mean Time Between Failures

MTBMA
Mean Time Between Maintenance Activities

Mult
Multipling

Multi Service Provisioning Platform (MSPP)
SONET Add/Drop Multiplexer Network Element with Ethernet/Data capability.

Multiplexer
A device (circuit pack) that combines two or more transmission signals into a combined signal on a shared medium.

Multiplexing
The process of combining multiple signals into a larger signal at the transmitter by a multiplexer. The large signal is then split into the original smaller signals at the receiver by a demultiplexer.

MUX
Multiplex

N **NA**
Not Applicable

NARTAC
North American Regional Technical Assistance Center

NE
network element

NE ACTY
Near-End Activity

Near End
The network element the user is at or is working on. Also called local.

NEBS
Network Equipment-Building System

Network Element (NE)
A node in a telecommunication network that supports network transport services and is directly manageable by a management system.

Network Service Access Point (NSAP) Address
Network Service Access Point Address (used in the OSI network layer 3). An automatically assigned number that uniquely identifies a network element for the purposes of routing DCC messages.

Network Time Protocol
Network time protocol is an easy, accurate, and automatic method to get and synchronize date/time.

NIC
Network Interface Card

nm
Nanometer (10^{-9} meters)

NMA
Network Monitoring and Analysis

NMON
Not Monitored (provisioning state)

No Request State

This is the routine-operation quiet state in which no external command activities are occurring.

Node

A network element in a ring or, more generally, in any type of network. In a network element supporting interfaces to more than one ring, node refers to an interface that is in a particular ring. Node is also defined as all equipment that is controlled by one system controller. A node is not always directly manageable by a management system.

Nonpreemptible unprotected traffic (NUT)

Traffic carried on (working and/or protection) BLSR channels for which protection switching has been provisioned as disabled. NUT must be employed when using an alternate protection scheme for data such as RSTP. As the name implies, NUT is unprotected and not preempted in the event of a protection switch. NUT carried on nonpreemptible unprotected channels affords a higher level of survivability as compared to extra traffic, which is preempted during a protection switch, but a lower level of survivability as compared to working traffic, which is carried on its corresponding protection channel during a protection switch.

Nonrevertive Switching

In nonrevertive switching, an active and standby line exist on the network. When a protection switch occurs, the standby line is selected to support traffic, thereby becoming the active line. The original active line then becomes the standby line. This status remains in effect even when the fault clears. That is, there is no automatic switch back to the original status.

Nonvolatile Memory (NVM)

Memory that retains its stored data after power has been removed. An example of NVM would be a hard disk.

Not Monitored (NMON)

A provisioning state for equipment that is not monitored or alarmed.

NR

Not Reported

NRZ

Nonreturn to Zero

NSA

Not Service Affecting

NSAP Address

Network Service Access Point Address (used in the OSI network layer 3)

NTF

No Trouble Found

NTP

Network time protocol

NUT

Nonpreemptible unprotected traffic

NVM

Non-Volatile Memory

O

OAM&P

Operations, Administration, Maintenance, and Provisioning

OC-1

Optical Carrier, Level 1 Signal (51.84 Mb/s)

OC-12

Optical Carrier, Level 12 Signal (622.08 Mb/s)

OC-192

Optical Carrier, Level 192 Signal (9953.28 Mb/s) (10 Gb/s)

OC-3

Optical Carrier, Level 3 Signal (155.52 Mb/s)

OC-48

Optical Carrier, Level 48 Signal (2488.32 Mb/s) (2.5 Gb/s)

OC, OC-n - Optical Carrier

The optical signal that results from an optical inversion of an STS signal; that is, OC-1 from STS-1 and OC-n from STS-n.

OCH

Optical Channel

OI

Operations Interworking

OLIU

Optical Line Interface Unit

OOF

Out of Frame

OOL

Out of Lock

OOS

Out-of-Service

Open Systems Interconnection (OSI)

Referring to the OSI reference model, a logical structure for network operations standardized by the International Standards Organization (ISO).

Operations Interface

Any interface providing you with information on the system behavior or control. These include the equipment LEDs, SYSCTL faceplate, WaveStar CIT, office alarms, and all telemetry interfaces.

Operations Interworking (OI)

The capability to access, operate, provision, and administer remote systems through craft interface access from any site in a SONET/SDH network or from a centralized operations system.

Operations System (OS)

A central computer-based system used to provide operations, administration, and maintenance functions.

OPS/INE

Operations System/Intelligent Network Element

Optical Channel (OCH)

The top layer of the DWDM network that provides transport of client signals (for example, SONET, 1GE, OTU2). The OCH layer is comparable in function to the SONET path layer.

Optical Channel Transport Unit 2 (OTU2)

The OTU2 is the information structure used for transport over one or more optical channel connections. It consists of the optical channel data unit and OTU2 related overhead (FEC and overhead for management of an optical channel connection). It is characterized by its frame structure, bit rate, and bandwidth.

Optical Transport Network (OTN)

Network used to transport user signals via ITU compliant wavelengths. The OTN is composed of the OTU2, OCH, and OTS layers.

Optical Transport Section (OTS)

The lowest layer of the OTN that provides physical transport. The OTS layer is terminated on an OTS terminating equipment. The OTS layer is comparable in function to the SONET section layer.

OS

Operations System

OSI

Open Systems Interconnection

OSMINE

Operations Systems Modifications for the Integration of Network Elements

OSP
Outside Plant

OTN
Optical Transport Network

OTS
Optical Transport Signal

OTU2
Optical Channel Transport Unit 2

P

P-bit
Performance Bit

Pass Through
Paths that are cross-connected directly across an intermediate node in a ring network.

Path
A logical connection between the point at which a standard frame format for the signal at the given rate is assembled, and the point at which the standard frame format for the signal is disassembled.

Path Protection Group
The part of a cross-connection topology that is provisioned to provide path-level protection switching for all the constituent signals carried by the cross-connection. A path protection group can be identified as an entity by its logical output tributary and its cross-connection rate. A path protection group consists of one or more constituent path selectors.

PC
Personal Computer

PCMCIA
Personal Computer Memory Card International Association

Peak Information Rate Policer
The peak information rate policer meters packet traffic leaving the internal packet switch and going toward the SONET network. If the packets exceed the provisioned peak information rate, the packets are dropped.

Performance Monitoring (PM)
Measures the quality of service and identifies degrading or marginally operating systems (before an alarm would be generated).

PID
Program Identification

Pipe Mode

Alcatel-Lucent 1665 DMX supports cross-connections on adaptive rate OC-n ports (pipe mode). The signal rates adapt to the supported set of signal rates. Cross-connections may be provisioned at any cross-connection rate that is supported for the tributaries associated with the OC-n ports. A cross-connection can carry any set of constituent signals; however, the total of the constituent signal rates must not exceed the cross-connection rate. Fault monitoring and performance monitoring occur on the accepted incoming rates.

PIR

Peak information rate

PJC

Pointer Justification Count

Plesiochronous Network

A network that contains multiple maintenance subnetworks, each internally synchronous and all operating at the same nominal frequency, but whose timing may be slightly different at any particular instant. For example, in SONET networks, each timing traceable to their own Stratum 1 clock are considered plesiochronous with respect to each other

PLL

Phase-Locked Loop

PM

Performance Monitoring

POP

Points of Presence

Port (also called Line)

The physical interface, consisting of both an input and output, where an electrical or optical transmission interface is connected to the system and may be used to carry traffic between network elements. The words "port" and "line" may often be used synonymously. "Port" emphasizes the physical interface, and "line" emphasizes the interconnection. Either may be used to identify the signal being carried.

Port Protection Group

A user provisioned association of protected optical interface ports. This association is used for line protection. The group of ports represent both a protection switching entity and also a set of lines that carry services to/from another network element. The port protection groups also determine the set of logical tributaries from and to which cross-connections can be provisioned.

Port State Provisioning

A feature that allows a user to suppress alarm reporting and performance monitoring during provisioning by supporting multiple states (automatic, in-service, and not monitored) for low-speed ports.

Ported Mode

In the Ported mode, a DS3 port receives and transmits a DS3 signal on the backplane electrical interface to the DSX.

Portless Mode

In the Portless mode, a DS3 port does not use backplane electrical connector. This mode is used to map a DS1 being received in a channelized DS3 within an STS1 into a VT, and vice versa. The DS1 is cross-connected at the VT1.5 level.

POTS

Plain Old Telephone Service

PRBS

Psuedo-random Bit Sequence

Proactive Maintenance

Refers to the process of detecting degrading conditions not severe enough to initiate protection switching or alarming, but indicative of an impending signal fail or signal degrade defect (for example, performance monitoring).

Protection

Extra capacity (channels, circuit packs) in transmission equipment that is not intended to be used for service, but rather to serve as backup against failures.

Protection Group

A logical grouping of ports or circuit packs that share a common protection scheme; for example, UPSR switching or 1+1 line.

PROTN

Protection

Provisioning

The modification of certain programmable parameters that define how the node functions with various installed entities. These modifications are initiated locally or remotely by either a CIT or an OS. They may arrive at the node via the IAO LAN, CIT port, or any DCC channel. The provisioned data is maintained in NVM and/or hardware registers.

PTM

Pluggable Transmission Module

PWR

Power

Q **QoS**

Quality of Service

R

RADIUS

Remote Authentication Dial In User Service

RAI

Remote Alarm Indication

RAM

Random Access Memory

RDI

Remote Defect Indication

Reactive Maintenance

Refers to detecting defects/failures and clearing them.

Remote

See Far-End (FE).

Remote Defect Indication (RDI)

An indication returned to a transmitting terminal that the receiving terminal has detected an incoming section failure. [Previously called far-end-receive failure (FERF).]

Remote Network Element

Any network element that is connected to the referenced network element through either an electrical or optical link. It may be the adjacent node on a ring or N nodes away from the reference. It also may be at the same physical location, but is usually at another (remote) site.

Revertive

A protection switching mode in which, after a protection switch occurs, the equipment returns to the nominal configuration (that is, the service equipment is active, and the protection equipment is standby) after the clearing of any failure conditions that caused a protection switch to occur or after any external switch commands are reset. See Nonrevertive.

RFI

Remote Failure Indication

Ring

A configuration of nodes comprised of network elements connected in a circular fashion. Under normal conditions, each node is interconnected with its neighbor and includes capacity for transmission in either direction between adjacent nodes. Path switched rings use a head-end bridge and tail-end switch. Line switched rings actively reroute traffic over a protection line.

Ring (0x1) Low-Speed Interface

Formerly referred to as dual 0x1 or single 0x1. In ring applications, Alcatel-Lucent 1665 DMX may use a 0x1 interface, meaning both fibers carry service, as opposed to a linear (1+1) low-speed interface where one fiber is used for service and other for protection. See 1+1.

RNE
Remote network element

Root node
The node from which path cost to any other node is measured.

RSTP
Rapid Spanning Tree Protocol

RTAC
Alcatel-Lucent Regional Technical Assistance Center (1-800-225-RTAC)

RTRV
Retrieve

RU
Rack Unit

RZ
Return to Zero

S

SA
Service Affecting

SARB
Status All Resources Busy

SARB Error
This error response indicates the condition “Status, All Resources Busy.”

SD
Signal Degrade

SEFS
Severely Errored Frame Seconds

Self-Healing
Ring architecture in which two or more fibers are used to provide route diversity. Node failures only affect traffic dropped at the failed node.

Service
The operational mode of a physical entity that indicates that the entity is providing service. This designation will change with each switch action.

SES
Severely Errored Seconds

Severely Errored Seconds (SES)

This performance monitoring parameter is a second in which a signal failure occurs, or more than a preset amount of coding violations (dependent on the type of signal) occur.

SF

Super Frame (format for DS1 signal)

SFP

Small Form Factor Pluggable - Type of pluggable transmission modules used for OC-3, OC-12, OC-48, and optical Ethernet/Data interfaces.

Shelf ID

A switch-settable parameter with values from 1 to 8. Used to log into a selected shelf in a bay using the CIT (does not apply to Alcatel-Lucent 1665 DMX).

Shelf View

A graphical depiction of one shelf. Selectable objects in this view are the shelf, the slots/circuit packs, and the ports.

SID

System Identification

Site ID

A switch-settable parameter with values from 1 to 8. Displayed on the SYSCTL circuit pack to indicate to which site the faceplate alarms and LEDs apply (does not apply to Alcatel-Lucent 1665 DMX).

SLA

Service Level Agreement

Slot

A physical position in a shelf for holding a circuit pack and connecting it to the backplane. This term is also used loosely to refer to the collection of ports or tributaries connected to a physical circuit pack placed in a slot.

SM

Single Mode

SMC

SONET Minimum Clock

SNMP

Simple Network Management Protocol

Software Backup

The process of saving an image of the current network element's databases, which are contained in its NVM, to a remote location. The remote location could be the WaveStar CIT or an OS.

Software Download

The process of transferring a software generic from a remote entity to the target network element's memory. The remote entity may be the WaveStar CIT or an OS. The download procedure uses bulk transfer to move an uninterpreted binary file into the network element.

SONET

Synchronous Optical NETwork

Spanning Tree Group

Nodes can be provisioned to belong to a spanning tree group. Only the nodes within that group participate in the spanning tree for the group.

SPE

Synchronous Payload Envelope

Squelch Map

This map contains information for each cross-connection in a ring and indicates the source and destination nodes for the low-speed circuit that is part of the cross-connection. This information is used to prevent traffic misconnection in rings with isolated nodes or segments.

Stand-alone shelf

A shelf that does not have provisioned sub-tending sub-shelves and is not provisioned to operate as a sub-shelf.

Standby

Standby identifies a protected entity which is not currently selected by the receiver at either end as the payload carrying signal hat is not currently carrying service. See Active.

Standing Condition

A standing condition (SC) is either an event (usually user initiated such as a switch request) or an alarm that is provisioned NA (Not Alarmed).

Status

The indication of a short-term change in the system.

STQ

Secondary Transit Queue

Stratum 3 Timing Generator

The timing generator circuit pack, located in the high-speed OLIU circuit pack, that generates clock signals for distribution to the transmit circuits. It operates in the free-running, line-timing, externally timed, and holdover modes.

STS-1 SPE

STS-1 Synchronous Payload Envelope

STS-1 SPE - STS-1 Synchronous Payload Envelope

A 125-µsec frame structure composed of STS path overhead and the STS-1 payload.

STS-12c

Synchronous Transport Level 12 Concatenated Signal

STS-192c

Synchronous Transport Level 192 Concatenated Signal

STS-3c

Synchronous Transport Level 3 Concatenated Signal

STS-3c

Synchronous Transport Level 3 Concatenated Signal. *See OC-3c*.

STS-48c

Synchronous Transport Level 48 Concatenated Signal

STS, STS-n

Synchronous Transport Signal

STS, STS-n - Synchronous Transport Signal

The basic building block signal with a rate of 51.840 Mb/s for an STS-1 signal and a rate of n times 51.840 Mb/s for an STS-n signal.

STU

Synchronized - Traceability Unknown

Sub-shelf

A shelf in a multi-shelf configuration that is provisioned to operate as a sub-tending sub-shelf.

Subnetwork

A group of interconnected/interrelated network elements. The most common connotation is a synchronous network in which the network elements have data communications channel (DCC) connectivity.

Superframe Format (SF)

A DS1 framing format in which 24 DS0 time slots plus a coded framing bit are organized into a frame which is repeated 12 times to form the superframe.

Suspend

Suspend refers to temporarily stopping an upgrade in progress.

Synchronization Messaging

SONET synchronization messaging is used to communicate the quality of network timing, internal timing status, and timing states throughout a subnetwork.

Synchronous Network

The synchronization of transmission systems with synchronous payloads to a master (network) clock that can be traced to a reference clock.

Synchronous Optical Network (SONET)

The North American standard for the rates and formats that defines optical signals and their constituents.

Synchronous Payload

Payloads that can be derived from a network transmission signal by removing integral numbers of bits from every frame. Therefore, no variable bit-stuffing rate adjustments are required to fit the payload in the transmission signal.

Synchronous Payload Envelope (SPE)

The combined payload and path overhead of an STS-1, STS-3c, STS-12c, STS-48c, , or STS-192c signal.

SYSCTL

System Controller (circuit pack)

SYSCTL - System Controller

The system controller circuit pack that provides overall administrative control of the terminal.

System View

A graphical depiction of the entire network element. Selectable objects in this view are the bays and shelves.

T

T1

A carrier system that transmits at the rate of 1.544 Mb/s (a DS1 signal).

T1X1 and T1M1

The ANSI committees responsible for telecommunications standards

T2

A carrier system that transmits at the rate of 6.312 Mb/s (a DS2 signal).

T3

A carrier system that transmits at the rate of 44.736 Mb/s (a DS3 signal).

TA

Telcordia ® Technical Advisory

Target Identifier (TID)

A provisionable parameter that is used to identify a particular network element within a network. It is a character string of up to 20 characters where the characters are letters, digits, or hyphens (-).

TARP

Target Identifiers Address Resolution Protocol

TBD

To Be Determined

TCA
Threshold-Crossing Alert

TCP/IP
Transmission Control Protocol/Internet Protocol

TDC
TARP Data Cache

TDM
Time Division Multiplexing

Telcordia ®
Telcordia ® is a well-recognized telecommunications' standards organization.

Test Access
A set of cross-connection topologies used in conjunction with a testing system to monitor and "split" signal paths for purposes of fault isolation.

Threshold-Crossing Alert (TCA)
A message type sent from a network element that indicates that a certain performance monitoring parameter has exceeded a specified threshold.

Through (or Continue) Cross-Connection
A cross-connection within a ring, where the input and output tributaries have the same tributary number but are in lines opposite each other.

Through Timing
Refers to a network element that derives its transmit timing in the east direction from a received line signal in the east direction and its transmit timing in the west direction from a received line signal in the west direction.

THz
Terahertz (10^{12} Hz)

TID
Target Identifier

Time Division Multiplexing (TDM)
A technique for transmitting a number of separate data, voice, and/or video signals simultaneously over one communications medium by interleaving a portion of each signal one after another.

Time Slot Assignment (TSA)
A capability that allows any tributary in a ring to be cross-connected to any tributary in any lower-rate, nonring interface or to the same-numbered tributary in the opposite side of the ring.

Time Slot Interchange (TSI)
A set of nodes configured as a ring with paths established in both directions of the ring. Switching occurs per-path at the drop nodes.

TIRKS
Trunks Integrated Records Keeping System

TL1
Transaction Language 1

TR
Telcordia ® Technical Requirement

Transaction Language One (TL1)
The permission level associated with each user login that defines which commands the user can execute.

Transparent Mode
In Transparent Mode, port tags (which are actually VLAN tags with a TPID value other than 8100hex) are used to separate traffic for different customers. A port tag is added to each incoming frame at the ingress LAN port. The port tag contains a provisionable customer ID and priority level.

Tributary
A path-level unit of bandwidth within a port, or the constituent signal(s) being carried in this unit of bandwidth; for example, an STS-1 tributary within an OC-N port.

TSA
Time Slot Assignment

TSI
Time Slot Interchange

TSO
Technical Support Organization

TSS
Technical Support Services

U

UAS
Unavailable Seconds

Unavailable Seconds (UAS)
In performance monitoring, the count of seconds in which a signal is declared failed or in which 10 consecutively severely errored seconds (SES) occurred, until the time when 10 consecutive non-SES occur.

Unidirectional Path-Switched Ring (UPSR)

Path-Switched rings employ redundant fiber optic transmission facilities in a pair configuration, with one fiber transmitting in one direction (for example, East) and the backup fiber transmitting in the other direction (for example, West). If the primary ring fails, then the protection ring takes over.

UPD/INIT

Update/Intialize

UPD/INIT

A push button on the SYSCTL faceplate.

UPSR

Unidirectional Path Switched Rings

User Privilege

Permits a user to perform on the computer system on which the system software runs.

V

VAC

Volts Alternating Current

VCG

Virtual Concatenation Group

VDC

Volts Direct Current

Virtual LAN (VLAN)

A virtual LAN (VLAN) is a subset of a LAN. A VLAN is created by putting VLAN IDs in packets that indicate membership to a VLAN of that ID. A Local Area Network (LAN) can have multiple VLANs within it, up to the number of IDs available. Members (ports) of different VLANs do not see the traffic of VLANs of which they are not members. A port may be a member of many VLANs (LAN ports in 802.1Q mode, WAN ports). In the Transparent mode, a LAN port is typically assigned membership to a single VLAN.

In Transparent mode, VLANs are assigned to ports using Port Tag (ed-eport and ed-vcg. In 802.1Q mode, VLANs are assigned to ports using VLAN IDs (ent-vlan/ed-vlan).

A VLAN tag is the specific field of information in a packet that carries the VLAN ID number.

Virtual Switch

A virtual switch is a grouping of ports on an Ethernet switch that results in partitioning of the switch into multiple "logical" switches. A port may only be a member of one virtual switch.

Virtual Tributary (VT)

A structure designed for transport and switching of sub-STS-1 payloads. There are currently four sizes: VT1.5 (1.728 Mb/s), VT2 (2.304 Mb/s), VT3 (3.456 Mb/s), and VT6 (6.912 Mb/s).

VLAN
Virtual Local Area Network

VLF
Very Large Fabric

VM
Violation Monitor

VMR
Violation Monitor and Removal

VoIP
Voice over Internet Protocol

VPN
Virtual Private Network

vslot
Virtual Slot

VT
Virtual Tributary

VT-G - Virtual Tributary Group
A 9-row by 12-column SONET structure (108 bytes) that carries one or more VTs of the same size. Seven VT groups (756 bytes) are byte-interleaved within the VT-organized STS-1 synchronous payload envelope

VT1.5
Virtual Tributary 1.5 (1.728 Mb/s)

VT1.5 Tributary
A SONET logical signal with a data rate of 1.728 Mb/s. In the 9-row structure of the STS-1 SPE, a VT1.5 occupies three columns. VT-structured STS-1 SPEs are divided into seven VT groups. Each VT group occupies 12 columns of the 9-row structure and, for VT1.5s, contains four VTs per group.

W

Wait to Restore Time (WRT)
Corresponds to the time to wait before switching back after a failure has cleared (in a revertive protection scheme). The WRT can be between 0 and 12 minutes, in increments of 1 minute.

Wait-to-Rename
Wait to Rename timer for Optimized 1+1 optical line protection. After a protection switch clears, the system waits the provisioned length of time before renaming the working section 1 and working section 2 as Primary and Secondary.

WAN

Wide Area Network

Wavelength Division Multiplexing (WDM)

A means of increasing the information-carrying capacity of an optical fiber by simultaneously transmitting signals at different wavelengths.

WDCS

Wideband Digital Cross-Connect System

WDM

Wavelength Division Multiplexing

Wide Area Network (WAN)

A communication network that uses common-carrier provided lines and covers an extended geographical area.

Wizard

A form of user assistance that automates a procedure through a dialog with the user.

WTR

Wait to Restore Time

X

XFP

10 Gb/s Small Form Factor Pluggable - Type of pluggable transmission modules used for OC-192 interfaces.

Z

Zero Code Suppression

A technique used to reduce the number of consecutive zeros in a line-codes signal (B3ZS for DS3 signals and B8ZS for DS1 signals).

Index