Alcatel SONET Multiplexer

1603 SMX
Maintenance and Trouble Clearing

PN 3AL03182ABAA 01
R03.01, Issue 1, October 2001

THIS PRODUCT COMPLIES WITH D.H.H.S. RADIATION PERFORMANCE STANDARDS 21 CFR, 1040.10, FOR A CLASS 1 LASER PRODUCT.

DANGER

Invisible laser radiation is present when the optic connector is open. AVOID DIRECT EXPOSURE TO BEAM.

WARNING

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 protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the 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 users will be required to correct the interference at their own expense.

NOTICE

The product specification and/or performance levels contained in this document are for information purposes only and are subject to change without notice. They do not represent any obligation on the part of Alcatel. Such obligations will only be committed to in a written sales agreement signed by Alcatel USA. In addition, release notes describing revisions to software may impact information in this document.

DOCUMENTATION

To offer comments on this documentation, email TND.Documentation_usa@alcatel.com, fax 972-519-4701, or write to the following address.

Alcatel USA
Attention: Doc Comment, MS PRODS
1000 Coit Road
Plano, Texas 75075-5813 USA

1603 SMX Maintenance and Trouble Clearing Table of Contents

Introduction

Task Index List (IXL)

Routine Task Procedures (RTP)

Trouble Analysis Data (TAD)

Trouble Analysis Procedures (TAP)

Detailed Level Procedures (DLP)

Training (TNG)

Introduction

1. How To Use TOP Documentation

Overview

1.1 This manual is a Task-Oriented Practice (TOP). It is a programmed document that gives step-by-step instructions to do a job (or task). Whenever this manual is used, a task is to be performed that requires accomplishing a result. The Master Task Index List or the Table of Contents is the starting point. They list task categories with references to a procedure to accomplish a task.

1.2 A TOP contains all the instructions needed to do a job. If a user is experienced on a particular job, a TOP provides just the information needed to do the job. If a user is doing the job for the first time, step-by-step instructions are given with enough detail to eliminate guessing.

1.3 TOP documentation is constructed in layers, separated by tabs that consist of the following (all layers may not be present in any one manual):

- Table of Contents
- Task Index List (IXL)
- Non-Trouble Procedure (NTP)
- Trouble Analysis Procedure (TAP)
- Detailed Level Procedure (DLP)
- Alcatel Job Aid (AJA)
- Routine Task List (RTL)
- Routine Task Procedure (RTP)
- Trouble Analysis Data (TAD)
- Training (TNG)

1.4 These layers provide the user with easy access to any point within the task description. The Table of Contents shows the current issue level of all procedures within the TOP document. The IXL (where to find) references all layers: NTP and TAP (what to do), DLP (how to do), RTL and RTP (what to do and how to do routine maintenance), and TAD and TNG (supporting information).

1.5 The TOP documentation is typically presented in text step procedures. Data organization is shown in Figure 1. The following paragraphs give a brief description of each layer used in the TOPs documentation.

Task Index List (IXL)

1.6 This layer lists each task described in the TOP document. To make it easier to find a task, the tasks are split into groups of similar tasks and placed in different IXLs, where applicable. A Master Task Index List provides a reference to the IXLs with titles indicating the functional grouping.

Trouble Clearing

1.7 Trouble clearing procedures can be classified into two broad job categories: Trouble Clearing (TAP) and Non-Trouble Clearing (NTP). The following are TOP definitions of these two types of work.

1.8 Trouble clearing procedures clear and repair trouble in the system. Trouble clearing can be to answer a customer complaint or in response to an office alarm, a trouble report, or an abnormal display.

1.9 Assume an alarm message was reported on a terminal or a visual alarm was indicated. The first step is to obtain the Maintenance and Trouble Clearing Manual. In it, locate the Master Task Index List and find the general task associated with the alarm under the "Find The Job In The List Below" heading. Once found, the associated index under the "Then Go To" heading directs a user to other procedures to choose from to clear the alarm in question. After the specific task is found under "Find The Job In The List Below" heading, locate the associated procedure under the "Then Go To" heading and go to it to follow a procedural flow to resolve the alarm.

1.10 Within a TAP, there may be references to other procedures (DLPs or TAPs), as required to clear the fault and return the system or unit to service.

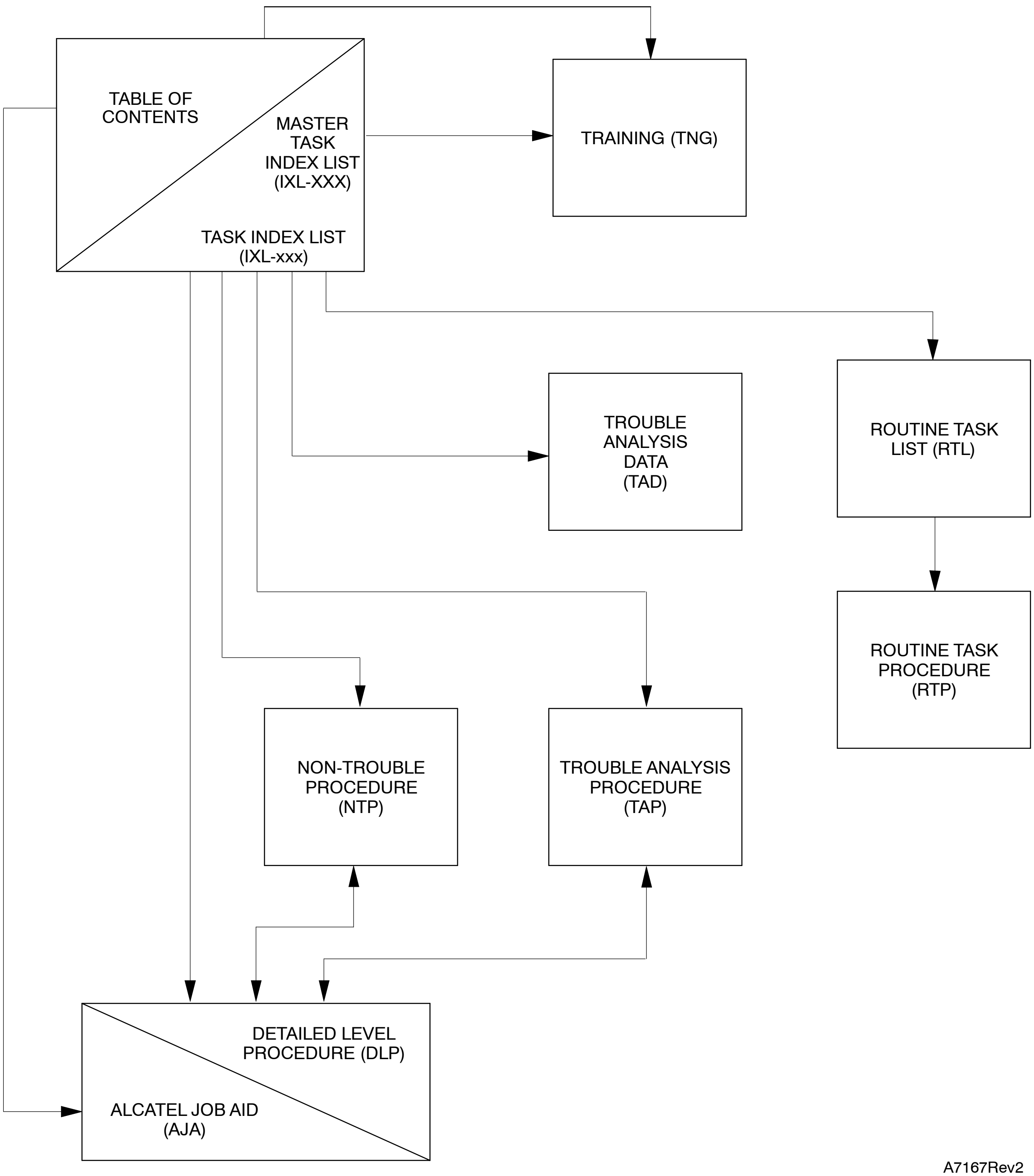


Figure 1. TOP Documentation Data Organization

Non-trouble Clearing Procedures (NTP)

1.11 Non-trouble clearing procedures are not connected with trouble clearing. NTPs are performed to accept a system after it has been installed, turn up a system for service, and maintain a system according to a controlled maintenance plan. Access to non-trouble clearing procedures is the same as trouble clearing procedures. An IXL is used to find a task category and the applicable procedure is selected to perform a task.

Trouble Analysis Procedure (TAP)

1.12 This element contains, in sequence, the steps required to perform a trouble clearing task to its completion. It tells the user WHAT TO DO to complete a task. The TAP may refer to another TAP. In most cases, the user does not return to the TAP after leaving it. For inexperienced or experienced personnel who want more information, some tasks provide a reference to a DLP or TNG section. After completing the referenced DLP or TNG, return to the same step in the TAP and continue the procedure.

Detailed Level Procedures (DLP)

1.13 This layer contains detailed support text steps that describe how to perform a procedure. In addition to step-by-step information, a DLP contains any tables or illustrations that may be required to perform the procedures. An example of a textual step procedure is shown in Figure 2.

1.14 The DLPs are typically referenced from an NTP or TAP, but references are also made from the IXL or other DLPs. When a DLP is referenced from a given point, the task in the referenced DLP may be performed. When the task is completed, the user returns to the point where the DLP was referenced.

Alcatel Job Aid (AJA)

1.15 AJAs are job oriented (task driven) and are divided into logical procedures permitting a division of labor or logical stopping points.

Routine Task List (RTL) / Routine Task Procedure (RTP)

1.16 The RTL contains a listing of routine tasks to perform routine maintenance, and refers the user to a Routine Task Procedure (RTP) for each task.

3AL03182AAAA
Issue 1, June 2001

DLP-519
Page 1 of 1

DLP-519
Retrieve/Change DS3 Format Parameter

Purpose

This procedure describes how to retrieve the provisioned value for the DS3 Format parameter and if necessary how to change the parameter.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select DS3. *NOTE: If T3 is connected to an LIF601, expand DS3 / DS1 TransMux after expanding Facility; then select DS3.*
2	In the result pane, right-click DS3 facility reporting alarm to display a context menu.
3	From the context menu, select **Provision Parameters** to display a Provision Parameters work view.
4	On the work view, note provisoned value of DS3 Format parameter.
5	Do you want to change DS3 Format parameter? If yes, go to step 6. If no, then go to step 8.
6	From DS3 Format drop-down list, select a new format value.
7	On the toolbar, select Submit icon.
8	Close work review.
9	STOP. This procedure is complete.

Retrieve/Change DS3 Format Parameter x-xx

AA2405

Figure 2. Format Example

Trouble Analysis Data (TAD)

1.17 TADs contain information to be used as a trouble clearing aid other than procedural data. It may be a functional schematic, text, or trouble clearing chart.

Training (TNG)

1.18 This layer contains information to give the user supplementary information, if necessary, to perform a given task.

General

1.19 Instructions are typically presented in a step format and decision steps are in the go-to structure (see Figure 2).

1.20 The completion of a specific procedure is stated simply.

1.21 The user should return to the task list or task summary list where this procedure was referenced to fully complete the job task.

Admonishments

1.22 Always do a job safely. The three admonishments to heed in TOPs, typically appearing as numbered steps, are:

DANGER **Possibility of personal injury.**

CAUTION **Possibility of service interruption.**

WARNING ***Possibility of equipment damage.***

References

1.23 Some procedural steps may contain notations that refer to additional information. Additional information may be notes, tables, figures, examples, and other procedures.

1.24 As shown in the following example, all mandatory information that is required to complete the step is shown as a separate phrase at the beginning of the step. All optional information, which can be accessed according to experience level, is enclosed in parentheses:

Refer to Table A. Mount tape. (For details, go to DLP-500.)

2. Documentation Summary

2.1 Refer to Table A for a summary of 1603 SMX R03.01 documentation.

Table A. 1603 SMX R03.01 Documentation

TITLE	DESCRIPTION
CD-ROM	
1603 SMX Electronic Documentation Library P/N 3AL03177ABAA	Provides standard and some optional manuals on CD-ROM; full display of documents formatted with integrated text and graphics, hyperlinked text for easy navigation, full-text search across all manuals, electronic notes, bookmarks, zooming, printing, and online help.
Online Troubleshooting Guide (OTG)	
Electronic Online Troubleshooting Guide (1301 NMX OTG1603) P/N 3AL02693AEAB (CD)	Provides online information to isolate and clear alarms and conditions generated by the 1603 SMX. The information is organized by topic windows.
Standard Documentation	
Product Information P/N 3AL03178ABAA	Provides general descriptions, applications, engineering information, and ordering guide for the 1603 SMX product, as well as information concerning ancillary equipment.
Installation Practices P/N 3AL03179ABAA	Provides step procedure instructions for unpacking, inspection, assembling, mounting, and wiring bays, shelves, ancillary items and cabling.
Turn-up P/N 3AL03180ABAA	Procedures, using 1301 NMX (PC USI), for optioning and installing plug-ins, provisioning the system, turning up circuits and testing the equipment to ensure it is ready for service; used in conjunction with 1301 NMX online help.
Maintenance and Trouble Clearing P/N 3AL03182ABAA	Provides Task Oriented Practices (TOP) for routine maintenance and trouble clearing to the plug-in level.
Provisioning Guide P/N 3AL03185ABAA	Provides step procedure instructions to provision hardware and facility parameters, backup system files, monitor performance, and general user functions.

Table A. 1603 SMX R03.01 Documentation (cont)

TITLE	DESCRIPTION
Optional Manuals	
Commands and Messages P/N 3AL03183AAAA	Provides reference information and detailed explanations for all product-specific commands and messages. This manual is designed to assist the craftsperson in working with TL1.
A Guide to Upgrading P/N 3AL03184ABAA	Provides in-service procedures to upgrade existing 1603 SMX systems using 1301 NMX.

3. TECHNICAL ASSISTANCE CENTER

3.1 The support provided by the Alcatel Technical Assistance Center (TAC) includes:

- Telephone assistance during normal working hours for routine and emergency service
- Telephone assistance after-hours for emergency and non-emergency service
- On-site technical support
- Software upgrade service
- Manufacturing-discontinued product support

3.2 Alcatel recommends that customers' craftpersons and maintenance personnel be trained by Alcatel and that these individuals be equipped with adequate test equipment, spares, and documentation at the site.

3.3 Effective and rapid troubleshooting requires that TAC personnel have dial-in modem access to customer equipment; therefore, it is recommended that customers equip systems with modem access.

Telephone Assistance During Normal Working Hours

3.4 The TAC staff is specialized by product family and is knowledgeable about current and past Alcatel products. The following tables list telephone numbers of specific engineering groups. Call during normal working hours: weekdays (excluding holidays) from 8:00 A.M.. to 5:00 P.M., CST in Plano, Texas. Refer to table A for TAC telephone numbers.

Table A. TAC

PRODUCT AREA	TELEPHONE NUMBER
Main Number	(888) 252-2832
Canada (All Systems)	(905) 873-6300
International Customers	(888) 252-2832 or (972) 519-4141
Cross-Connect Systems (Designated 1630 SX, 1631 SX, 1633 SX, 1641 SX)	(888) 252-2832
High Density Lightwave Systems (Designated 1648 SM, 1641 SM, 1651 SM, 1664 SM)	(888) 252-2832
Microwave Systems (Designated DST, MDR, RDI)	(888) 252-2832
Multiplex Systems (Designated DML, DMX)	(888) 252-2832
Operational Support Systems (Designated TSM, 1301 NM, 1320 NM, 1353 NM, 1354 NM)	(888) 252-2832
Optical Networks (Designated 1610 OA, 1640 OADM, 1680 OGM, 1690 OADM)	(888) 252-2832
SONET/Multiplexer Systems (Designated 1603 SM, 1603 SE)	(888) 252-2832

Emergency After-hours Telephone Assistance

NOTE *Emergency is defined as an out-of-service traffic-affecting problem or a nonoperating alarm system on traffic-bearing systems.*

3.5 After-hours telephone assistance with emergencies is available through Alcatel dispatch operators. Call **888-252-2832** and ask for the Lightwave, Microwave, Network Management, or Digital Cross-Connect/Switching emergency duty engineer. In Canada call **(905) 873-6300** 24 hours a day, 7 days a week.

Non-emergency After-hours Telephone Assistance

NOTE *Non-emergency is defined as installation turn-ups, application questions, traffic cutover, or routine maintenance.*

3.6 After-hours telephone assistance with non-emergency issues is best served when adequate documentation and resources are planned to address the issues. For this reason, Alcatel asks customers to prearrange non-emergency after-hours telephone support with TAC management.

3.7 Non-emergency after-hours telephone services are considered billable to the customer.

On-site Technical Support

3.8 On-site technical support for systems carrying traffic is available on request when services cannot be rendered effectively by telephone. Make requests for on-site technical support directly to TAC management.

3.9 On-site services are considered billable to the customer. Contact TAC for on-site service rates.

NOTE *Installation turn-up requests should be made to Installation and Test Services.*

Software Upgrade Service

3.10 Software upgrade service includes a remote pre-upgrade audit to ensure proper system operation, pre-upgrade backup, and a detailed, step-by-step procedure. This normally requires one or two days on site. Contact TAC for upgrade prices.

Manufacturing-discontinued Product Support

3.11 Telephone and on-site support is guaranteed for current products or products on Additions and Maintenance (A&M) status. For products on Manufacturing-discontinued (MD) status, services and rates vary depending on the age of the product and available material.

3.12 MD product support is billed by the hour. Contact TAC for more information.

4. INSTALLATION AND TEST SERVICES

4.1 The people most qualified to install and test equipment or systems are the people who build them. The staff professionals of Installation and Test Services thoroughly understand all requirements of Alcatel products and how to effectively install them. For further information, contact an Alcatel sales representative.

5. TECHNICAL TRAINING CENTER

5.1 Equipment training is available to all customers. Regularly scheduled courses are available at the training facility in Plano, Texas. For course schedules and rates, refer to the current Product Training Catalog, available at Alcatel's web site: www.usa/alcatel.com/telecom/service/catalog. Or call **(800) 372-5951** during normal working hours. To make course reservations, fax a completed Alcatel Technical Training Enrollment form (at the front of the Product Training Catalog) and a copy of the purchase order to **(800) 284-7701**.

5.2 To arrange on-site classes, call **(800) 372-5951** during regular working hours. To arrange custom and special training classes send requests, including a detailed description of training requirements, to the following address:

Alcatel USA Customer Training Center
ATTN: Registrar
1000 Coit Road
M/S 553
Plano, TX 75075-5813

The Technical Training Center will respond with a proposal of a training program to fulfill the request, the course development cost, and a preparation/presentation timetable.

6. REPLACEMENT/REPAIR SERVICES

6.1 Alcatel USA has established procedures for the replacement and repair of defective equipment, in-warranty or out-of-warranty. Units are repaired and returned promptly. The average turnaround time for repairs at Alcatel facilities is 10 calendar days (30 days for Manufacturing-discontinued (MD) products, subject to parts availability).

6.2 Emergency Advance Replacement is available: Alcatel ships the replacement unit within 24 hours of receiving the request. For out-of-warranty units, Emergency Advance Replacement fees are added to normal repair charges apply.

6.3 Follow this procedure when returning equipment:

1. With the unit(s) to be repaired, include:
   - Company name, billing and shipping address, phone number, and name of person(s) to contact in case of questions
   - Description of all known facts as to the nature of the failure(s)
   - Purchase order number or requisition number
   - Type number, part number, description of unit, and quantity to be repaired
   - Description of any additional repair action requested
2. Call Return and Repair at **(800) 372-1503** for the following:
   - Return Authorization (RA) number
   - Emergency Order
   - Advance Replacement
   - Return Address

   The RA number must be prominently marked on shipping label, the packing list, and any correspondence regarding the order.

7. QUALITY HOTLINE

7.1 In addition to the customer service telephone numbers, a toll-free 800 number is available to all customers to report quality issues related to products or services.

7.2 The 800 number is answered 24 hours a day, 365 days a year and is available throughout all 50 states and Canada.

7.3 An operator records the information and has an Alcatel Quality Assurance representative respond during normal business hours (8:00 a.m. to 5:00 p.m. CST, Monday through Friday). The regular customer service numbers should be used for normal customer service functions.

Quality Hotline: 800-553-4056

NOTE *All trademark notices listed in Table B may not apply to this manual.*

Table B. Trademark Notices

PRODUCT	TRADEMARK NOTICE
Contact Renu	Contact Renu is a registered trademark of Miller Stephenson.
Digital Earth Tester	Digital Earth Tester Megger (DET6D) is a registered trademark of AVO International.
Hayes Modem	Hayes Modem is a registered trademark of Hayes Microcomputer Products, Inc.
Ideal No-Ox	Ideal No-Ox is a trademark of Sanchem Inc.
Kim-wipe	Kim-wipe is a registered trademark of Kimberly-Clark.
Microcom	Microcom is a registered trademark of Microcom Corporation.
Microsoft	Microsoft is a registered trademark of Microsoft Corporation.
MNP	MNP stands for Microcom Networking Protocol and is a registered trademark of Microcom Corporation.
MS Access	MS Access is a trademark of Microsoft Corporation.
MS-DOS	MS-DOS is a trademark of of Microsoft Corporation.
Multitech	Multitech is a registered trademark of MultiTech Systems, Inc.
NO-OX-ID	NO-OX-ID is a registered trademark of Sanchem, Inc.
OpenView	OpenView is a registered trademark of Hewlitt-Packard.
WECO	WECO is a trademark of AT&T.

Table B. Trademark Notices (cont)

PRODUCT	TRADEMARK NOTICE
Windows	Windows is a trademark of Microsoft Corporation.
Windows 2000	Windows 2000 is a registered trademark of Microsoft Corporation.
Windows 95	Windows 95 is a registered trademark of Microsoft Corporation.
Windows 98	Windows 98 is a registered trademark of Microsoft Corporation.
Windows NT	Windows NT is a registered trademark of Microsoft Corporation.

IXL-001
Task Index List

FIND THE JOB	THEN GO TO...
Automatic Download...Allow	DLP-527
BITS Alarm (Input)...Clear	TAP-012
BITS Frame Format and Line Code Parameters...Retrieve/Change	DLP-539
BLSR Alarm...Clear	TAP-058
BLSR Ring Parameters...Retrieve/Change	DLP-543
BLSR Sequence Map...Retrieve/Change Provisioning of	DLP-563
Change Alarm Notification Code	DLP-534
Change ATM Port PM Threshold Levels	RTP-002
Change ATM Processor PM Threshold Levels	RTP-002
Change PM Mode	RTP-002
Change PM Threshold Levels	RTP-002
Change POS Port PM Threshold Level	DLP-574
Change Traffic Descriptor Characteristics	DLP-530
Check Fans and Filters	RTP-001
Check Version of Software/Firmware Installed on a Unit	DLP-521
Clean Fibers	DLP-012
Clear AAL5 Alarm	TAP-055
Clear Alarms Using Visual Indicators	TAP-010
Clear ATM Port Alarm	TAP-051
Clear ATM Processor Alarm	TAP-052
Clear BITS Alarm (Input)	TAP-012
Clear BLSR Alarm	TAP-058
Clear (COM) Common NE Alarm	TAP-016
Clear Craft Communication Loss	TAP-039
Clear Command Equipage Errors (Exxx)	TAP-007
Clear Command Input Errors (Ixxx)	TAP-004
Clear Command Privilege Errors (Pxxx)	TAP-005
Clear Command Status Errors (Sxxx)	TAP-006
Clear DS1 Facility Alarm (External T1 Facility on DMIxxx)	TAP-035
Clear DS1 Facility Alarm (DS3/DS1 Transmux)	TAP-050
Clear EC1 Alarm	TAP-022
Clear ENV Alarm	TAP-020
Clear Equipment (EQPT) Alarm	TAP-021
Clear Error Messages	TAP-003
Clear Fan Faults	TAP-024
Clear Far-End Alarm (Lighted REM ALM LED on COA)	TAP-041

FIND THE JOB	THEN GO TO...
Clear Fuse and Alarm Panel (FAP) Alarm	TAP-025
Clear IP Tunnel Alarm	TAP-047
Clear LAN Alarm	TAP-044
Clear LLSDCC (EOC) Alarm	TAP-032
Clear LLSMLDCC (EOC) Alarm	TAP-045
Clear NE Sync (SYNCN) Alarm	TAP-027
Clear Network Alarm	TAP-018
Clear OCn (OC3, OC12, or OC48) Facility Alarm	TAP-029
Clear Output Sync Alarm (BITS Output)	TAP-013
Clear Port Alarm	TAP-017
Clear POS Port Alarm	TAP-059
Clear Power Distribution Unit (PDU) Alarm	TAP-048
Clear Remote (RMT) Alarm	TAP-031
Clear SML Facility Alarm	TAP-033
Clear STS (STS1, STS3c, or STS12c) Path Alarm	TAP-034
Clear T3 (DS3) Facility Alarm	TAP-043
Clear TADRMap Alarm	TAP-046
Clear USRLAN Alarm (LIF901)	TAP-056
Clear USRLAN Alarm (LIFG01)	TAP-057
Clear VCL Alarm	TAP-054
Clear VPL Alarm	TAP-053
Clear VT1.5 Path Alarm	TAP-038
Clear X.25 Alarm or X.25 Failure	TAP-023
Command Equipage Errors (Exxx) ... Clear	TAP-007
Command Input Errors (Ixxx) ... Clear	TAP-004
Command Privilege Errors (Pxxx) ... Clear	TAP-005
Command Status Errors (Sxxx)...Clear	TAP-006
Common (COM) NE Alarm...Clear	TAP-016
Connect PC or VDT to Craft 1 or Craft 2 Port	DLP-567
Copy Provisioning Database To/From COA or NEP	DLP-538
Copy Software Program (Local Only)	DLP-568
Craft Communications Loss...Resolve	TAP-039
Craft 2 Port Wiring...Orderwire, Serial E2A (TBOS) and...Verify	DLP-553
Create Entry in BLSR Manual Sequence Map	DLP-542
Cross-Connect...Retrieve, Create, Modify, or Delete	DLP-504

FIND THE JOB	THEN GO TO...
Delete TADRMap Pair	DLP-508
Determine/Change Payload Type	DLP-511
Determine Download Status of NE	DLP-526
Diagnostics...Allow	DLP-522
Direct Neighbors...Retrieve	DLP-560
Disable Monitoring of Section Trace	DLP-546
Download Software From Another NE...Remotely	DLP-569
Download Software to Directly Connected NE	DLP-570
Download Software From PC to Processor-Controlled Units	DLP-566
Download Status of NE...Determine	DLP-526
DS1 Facility Alarm (External T1 Facility on DMIxxx)...Clear	TAP-035
DS1 Facility Alarm (DS3/DS1 Transmux)...Clear	TAP-050
DS1 Frame Format and Line Code Parameters...Retrieve/Change	DLP-524
DS1 Loopback...Test	DLP-023
DS3 Format Parameter...Retrieve/Change	DLP-519
DS3 Loopbacks...Test	DLP-024
E2A Map Provisioning...Retrieve/Change	DLP-561
EC1 Alarm...Clear	TAP-022
Enhanced Remote Defect Indicator (ERDI)...Retrieve/Change	DLP-516
ENV Alarm...Clear	TAP-020
EQPT Alarm	TAP-021
Equalization Distance Parameter...Retrieve/Change	DLP-531
Equipment (EQPT) Alarm...Clear	TAP-021
Equipment PM Information...Retrieve	RTP-002
Equipment PM Registers...Initialize (Set to Zero)	RTP-002
Error Messages...Clear	TAP-003
Facility PM Information...Retrieve	RTP-002
Facility PM Mode...Change	RTP-002
Facility PM Mode Information...Retrieve	RTP-002
Facility PM Registers...Initialize (Set to Zero)	RTP-002
Facility PM Threshold Levels...Change	RTP-002
Facility PM Threshold Levels...Retrieve	RTP-002
Facility Switching...Release (Allow) Forced/Locked-Out	DLP-545
Fan Faults...Clear	TAP-024
Fans and Filters...Check	RTP-001
FAP Alarm ...Clear	TAP-025

FIND THE JOB	THEN GO TO...
Far-End Alarm (Lighted REM ALM LED on COA)...Clear	TAP-041
Fast Facility Protection (FFP) Switch...Allow	DLP-573
Fibers...Clean	DLP-012
Firmware...Allow Automatic Download of	DLP-532
Firmware...Manually Download	DLP-533
Forced/Locked-Out Facility Switch...Release (Allow)	DLP-545
FTP Backup of Provisioning Database...Perform	DLP-571
FTP Restoral of Provisioning Database...Perform	DLP-572
Handling Static-Sensitive Devices	DLP-518
Hardware Inventory...Retrieve	DLP-537
Identify Alarms Using 1301 NMX	TAP-001
Identify LDR501 Carrying Alarmed Path or Facility	DLP-565
Inhibit PM Reporting	DLP-510
Initialize (Set to Zero) ATM Port PM Registers	RTP-002
Initialize (Set to Zero) ATM Processor PM Registers	RTP-002
Initialize (Set to Zero) Equipment PM Registers	RTP-002
Initialize (Set to Zero) Facility PM Registers	RTP-002
Initialize (Set to Zero) Path PM Registers	RTP-002
Initialize (Set to Zero) POS Port PM Registers	RTP-002
Initialize (Set to Zero) Synchronization Registers	RTP-002
IP Tunnel Alarm...Clear	TAP-047
LAN Alarm...Clear	TAP-044
LAN Wiring...Verify/Connect	DLP-020
Laser...Restart	DLP-540
Line Buildout Parameter...Retrieve/Change Provisioning of	DLP-525
LLSDCC (EOC) Alarm...Clear	TAP-032
LLSMLDCC (EOC) Alarm...Clear	TAP-045
Log On/Log Off 1603 SMX Network Element (NE)	DLP-117
Logs...Retrieve/Initialize	DLP-528
Loopbacks...Allow Remote Activation of	DLP-548
Loopback...DS1...Test	DLP-023
Loopback...DS3...Test	DLP-024
Loopback...EC1...Test	DLP-025
Loopback...OC3...Test	DLP-026
Loopback...OC12...Test	DLP-027
Loopback...OC48...Test	DLP-030

FIND THE JOB	THEN GO TO...
Loopback Tests...Release	DLP-523
Lower Layer DCC Data...Retrieve/Change Provisioned	DLP-551
Maintenance Philosophy	TAD-001
Manual Area Address (MAADDR)...Provision	DLP-129
Manually Download Firmware	DLP-533
Manual Sequence Map (BLSR)...Create New Entry in	DLP-542
MTA101 Plug-in Unit...Test DS1/DS3 Facilities Using	DLP-022
NE Sync (SYNCN) Alarm...Clear	TAP-027
Network Alarm...Clear	TAP-018
Network Discovery...Perform	DLP-300
NSAPs...Retrieve	DLP-550
OCn Facility Alarm Alarm...Clear	TAP-029
Orderwire, Serial E2A (TBOS) and Craft 2 Port Wiring...Verify	DLP-553
Output Sync Alarm (BITS Output)...Clear	TAP-013
Path PM Information...Retrieve	RTP-002
Path PM Registers...Initialize (Set to Zero)	RTP-002
Path PM Threshold Levels...Change	RTP-002
Path PM Threshold Levels...Retrieve	RTP-002
Path Protection Switching...Release	DLP-507
Path Trace...Retrieve/Change Expected Incoming	DLP-512
Path Trace...Retrieve/Change Outgoing	DLP-514
Payload Type...Determine/Change	DLP-511
Perform FTP Backup of Provisioning Database	DLP-571
Perform FTP Restoral of Provisioning Database	DLP-572
Perform Network Discovery	DLP-300
Performance Monitoring	RTP-002
Plug-in Units...Replace	DLP-101
Plug-in Unit Status Indicators/Switches	TAD-002
PM Register Contents...Retrieve	DLP-517
PM Reporting...Allow	DLP-510
PM Information...Retrieve	RTP-002
PM Mode...Change	RTP-002
PM Registers...Initialize (Set to Zero)	RTP-002
PM Threshold Levels...Retrieve	RTP-002
Port Alarm...Clear	TAP-017
POS Port Alarm...Clear	TAP-059

FIND THE JOB	THEN GO TO...
POS Port PM Threshold Level...Change	DLP-574
Power Distribution Unit (PDU) Alarm...Clear	TAP-048
Processor...Restart	DLP-554
Protection Switching...OC3...Test	DLP-016
Protection Switching...OC12...Test	DLP-029
Protection Switching...OC48...Test	DLP-031
Protection Switching...Release Path	DLP-507
Provision Manual Area Address (MAADDR)	DLP-129
Provision NE for Telecommunications Management Network	DLP-128
Provisioning Database...Copy...To/From COA or NEP	DLP-538
Provisioning Database...Perform FTP Backup of	DLP-571
Provisioning Database...Perform FTP Restoral of	DLP-572
RAD Map Provisioning...Retrieve/Change	DLP-562
Release (Allow) Forced/Locked-Out Facility Switching	DLP-545
Release Loopback Tests	DLP-523
Release Path Protection Switching	DLP-507
Remotely Download Software From Another NE	DLP-569
Replace Plug-in Units	DLP-101
Resolve Craft Communications Loss	TAP-039
Restart Laser	DLP-540
Restart Processor	DLP-554
Retrieve Alarms/Conditions	DLP-100
Retrieve/Change ATM Cell Encapsulation	DLP-559
Retrieve/Change Provisioning for USRLAN Port	DLP-557
Retrieve/Change BITS Frame Format and Line Code Parameters	DLP-539
Retrieve/Change BLSR Ring Parameters	DLP-543
Retrieve/Change DS1 Frame Format and Line Code Parameters	DLP-524
Retrieve/Change DS3 Format Parameter	DLP-519
Retrieve/Change E2A Map Provisioning	DLP-561
Retrieve/Change Enhanced Remote Defect Indicator (ERDI) Parameter	DLP-516
Retrieve/Change Equalization Distance Parameter	DLP-531
Retrieve/Change Service State	DLP-501
Retrieve/Change Expected Incoming Path Trace	DLP-512
Retrieve/Change Expected Outgoing Path Trace	DLP-514
Retrieve/Change Expected Signal Label	DLP-509
Retrieve/Change Provisioned Lower Layer DCC Data	DLP-551

FIND THE JOB	THEN GO TO...
Retrieve/Change Provisioned Parameters	DLP-502
Retrieve/Change Provisioned Data for NE Environmental Alarms and Controls	DLP-552
Retrieve/Change BLSR Manual Sequence Map Provisioning	DLP-563
Retrieve/Change Provisioning of Line Buildout Parameter	DLP-525
Retrieve/Change Provisioning of Protection Switching Parameters	DLP-541
Retrieve/Change RAD Map Provisioning	DLP-562
Retrieve/Change Section Trace Data	DLP-547
Retrieve/Change Security Provisioning	DLP-520
Retrieve, Create, Modify, or Delete a Cross-Connect	DLP-504
Retrieve ATM Port PM Information	RTP-002
Retrieve ATM Port PM Threshold Levels	RTP-002
Retrieve ATM Processor PM Information	RTP-002
Retrieve ATM Processor PM Threshold Levels	RTP-002
Retrieve Equipment PM Information	RTP-002
Retrieve Facility PM Information	RTP-002
Retrieve Facility PM Mode Information	RTP-002
Retrieve Facility PM Threshold Levels	RTP-002
Retrieve Path PM Information	RTP-002
Retrieve Path PM Threshold Levels	RTP-002
Retrieve POS Port PM Information	RTP-002
Retrieve POS Port PM Threshold Levels	RTP-002
Retrieve Synchronization PM Data	RTP-002
Retrieve Hardware/Software Inventory	DLP-537
Retrieve/Initialize Logs	DLP-528
Retrieve NSAPs	DLP-550
Retrieve PM Register Contents	DLP-517
Retrieve Direct Neighbors	DLP-560
Retrieve Software Inventory	DLP-537
Ring Switch Exerciser...Allow Automatic	DLP-544
RMT Alarm...Clear	TAP-031
Run Equipment Diagnostics	DLP-500
Section Trace...Disable Monitoring of	DLP-546
Section Trace Data...Retrieve/Change	DLP-547
Security Provisioning...Retrieve/Change	DLP-520
SML Facility Alarm...Clear	TAP-033
Software Program (Local Only)...Copy	DLP-568

FIND THE JOB	THEN GO TO...
Software Inventory...Retrieve	DLP-537
Static-Sensitive Devices...Handling	DLP-518
Status Indicators/Switches...Plug-in Unit	TAD-002
STS Path Alarm...Clear	TAP-034
Switch a Working Unit to Protection	DLP-529
Switch OCn Facility	DLP-515
Switch Service Away from Alarmed Facility	DLP-513
Switch (and Release) to an Alternate Sync Source	DLP-503
Switch to a Redundant Unit	DLP-505
Synchronization Registers...Initialize (Set to Zero)	RTP-002
T3 (DS3) Facility Alarm...Clear	TAP-043
TADRMap Alarm...Clear	TAP-046
TADRMap Pair...Delete	DLP-508
TBOS (Serial E2A), Orderwire, and Craft 2 Port Wiring...Verify	DLP-553
Test Access Feature...Test DS1/VT1 Using	DLP-028
Test DS1/DS3 Facilities Using MTA101 Plug-in Unit	DLP-022
Test DS1/VT1 Using Test Access Feature	DLP-028
Test DS1 Loopback	DLP-023
Test DS3 Loopback	DLP-024
Test EC1 Loopback	DLP-025
Test OC3 Loopback	DLP-026
Test OC12 Loopback	DLP-027
Test OC48 Loopback	DLP-030
Test OC3 Protection Switching	DLP-016
Test OC12 Protection Switching	DLP-029
Test OC48 Protection Switching	DLP-031
Threshold Levels...Change	RTP-002
Threshold Level...Change POS Port PM	DLP-574
TMN...Provision NE for	DLP-128
Traffic Descriptor Characteristics...Change	DLP-530
USRLAN Alarm (LIF901)...Clear	TAP-056
USRLAN Alarm (LIFG01)...Clear	TAP-057
USRLAN Facility...Retrieve/Change Provisioning for	DLP-557
VCL Alarm...Clear	TAP-054
Verify/Connect LAN Wiring	DLP-020
Verify/Connect X.25 Port Wiring	DLP-019

FIND THE JOB	THEN GO TO...
Verify Orderwire, Serial E2A (TBOS) and Craft 2 Port Wiring	DLP-553
VPL Alarm...Clear	TAP-053
VT1.5 Path Alarm...Clear	TAP-038
X.25 Alarm or X.25 Failure...Clear	TAP-023
X.25 Port Wiring...Verify/Connect	DLP-019

RTP-001
Check Fans and Filters

Purpose

Provides procedures for checking fans and filters.

General

Fans are optionally equipped as needed per site requirements.

Equipment Required

Non-flammable heat source

Digital Volt Meter (DVM)

STEP	PROCEDURE
1	See Figure 1 to determine fan assembly location(s).
2	Refer to the fuse assignment chart on the Power Distribution Unit (PDU) or the Fuse and Alarm Panel (FAP) to identify fan fuse.
3	Verify that fan fuse is good; replace fuse if blown.
4	On the fan assemblies, set the NORMAL/DISABLE switch(es) to the NORMAL position.
5	Wait a few seconds for fans to start and stabilize.
6	Are all fans running? If yes, go to step 8. If no, apply heat to thermostat for a short time (see Figure 1 and refer to Table A); then go to step 7.
7	Do fans start running? If yes, go to step 8. If no, go to TAP-024 and clear trouble.

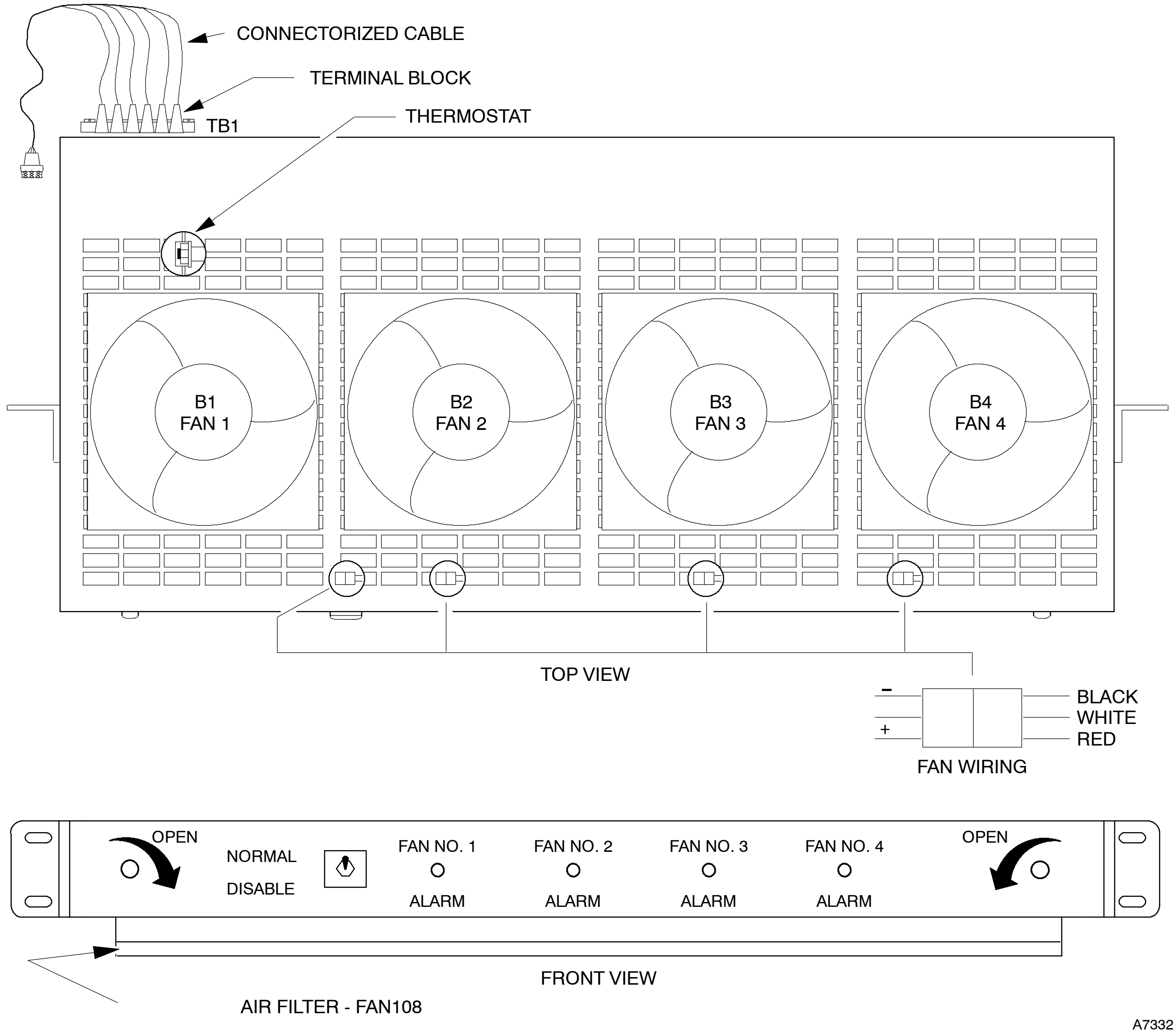


Figure 1. Fan Assembly Typical Layout

Table A. Fan On and Off Temperatures

MNEMONIC	GROUP	ON	OFF
FAN102	-002 without filter	38°C	29°C
FAN104	-004 with filter	38°C	29°C

8 Are any fan alarm LEDs (1-4) lighted on the fan assemblies?

If yes, go to TAP-024 and clear trouble.
If no, go to step 9.

9 **NOTE:** *Fans are thermostatically controlled to turn on and off (refer to Table A). If two fan assemblies are equipped, power is supplied to both assemblies through the thermostat in the top assembly. The fans can be forced on by applying heat to the top thermostat.*

Apply and remove heat. Verify that fans turn on and off as temperature rises and falls. (Refer to Table A.)

10 Do fans turn on and off?

If yes, go to step 11.
If no, go to TAP-024 and clear trouble.

11 Unlatch fan assembly and slide the assembly out.

12 Set the NORMAL/DISABLE switch to the DISABLE position.

13 Check air filter on Group-004 fan assembly and replace dirty filters with filters (PN 600044-641-001) per local practice.

14 Set the NORMAL/DISABLE switch to the NORMAL position and verify fan operation per step 9.

15 Slide fan assembly back into the shelf and secure the latches.

16 STOP. This procedure is complete.

RTP-002
Performance Monitoring

Purpose

This procedure describes how to perform various tasks pertaining to performance monitoring (PM) (e.g., how to retrieve PM information, how to initialize PM registers, how to set PM threshold levels, etc.)

General

Individual Performance Monitoring (PM) registers are used to store performance data that can be retrieved. This data is stored on a 15-minute increment basis for up to eight hours (or 32 consecutive 15-minute periods) and on a daily basis for the current and previous 24-hour period.

The types of performance data measured by the 1603 SMX are summarized in Figures 1 through 10.

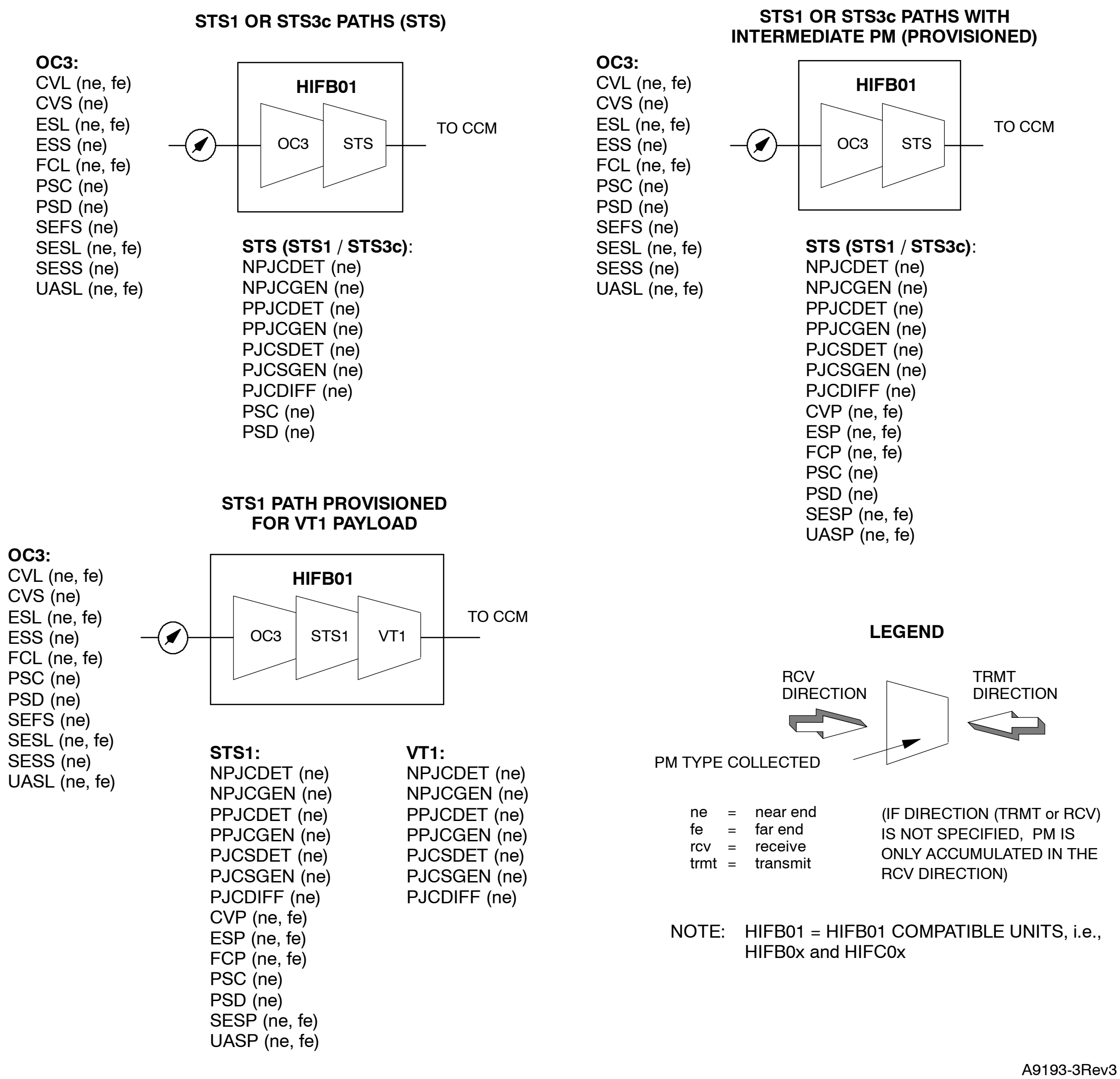


Figure 1. Performance Monitoring (PM) of OC3 Equipped Line Groups (HIFB01)

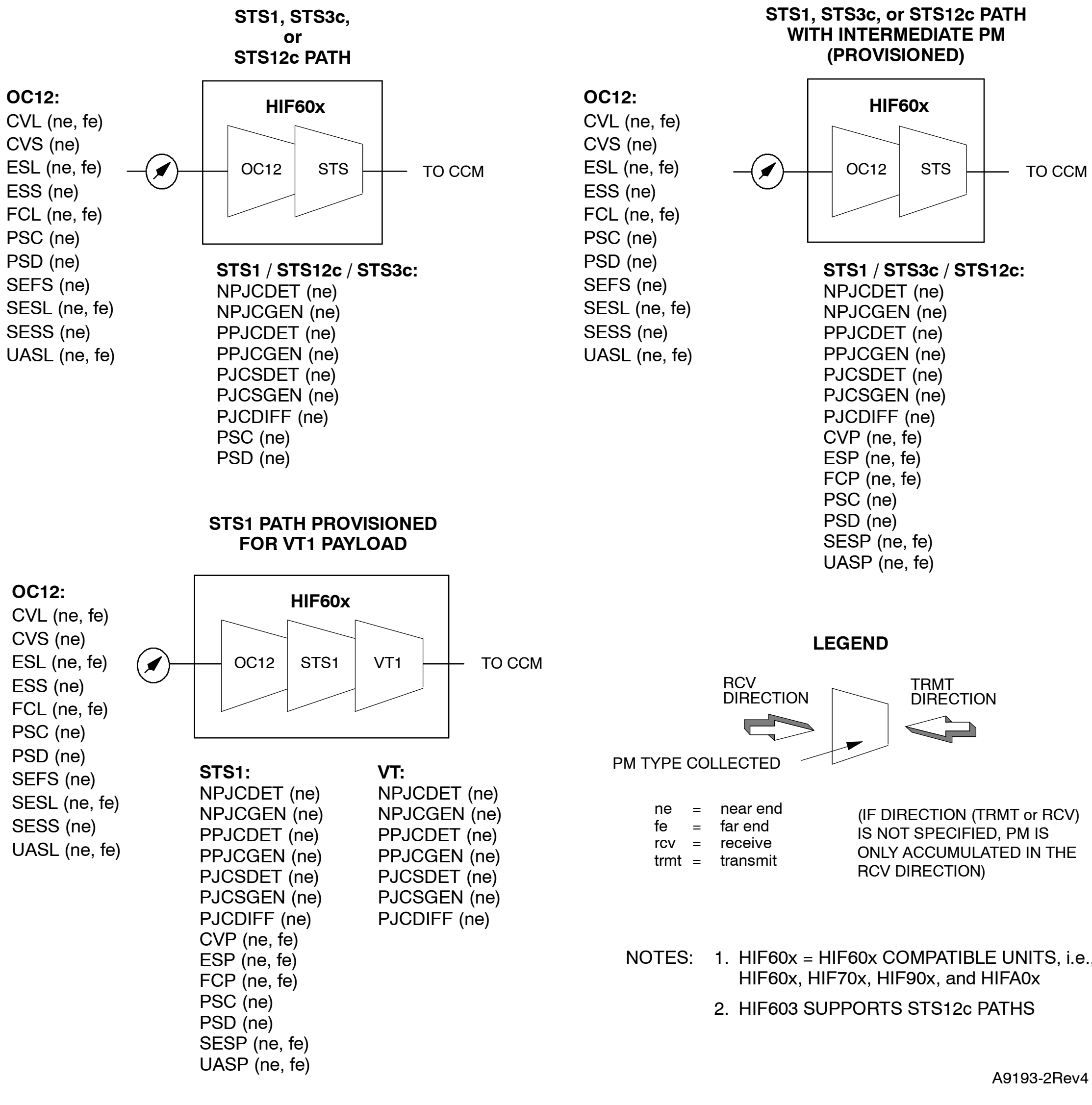


Figure 2. Performance Monitoring (PM) of OC12 Equipped Line Groups (HIF60x)

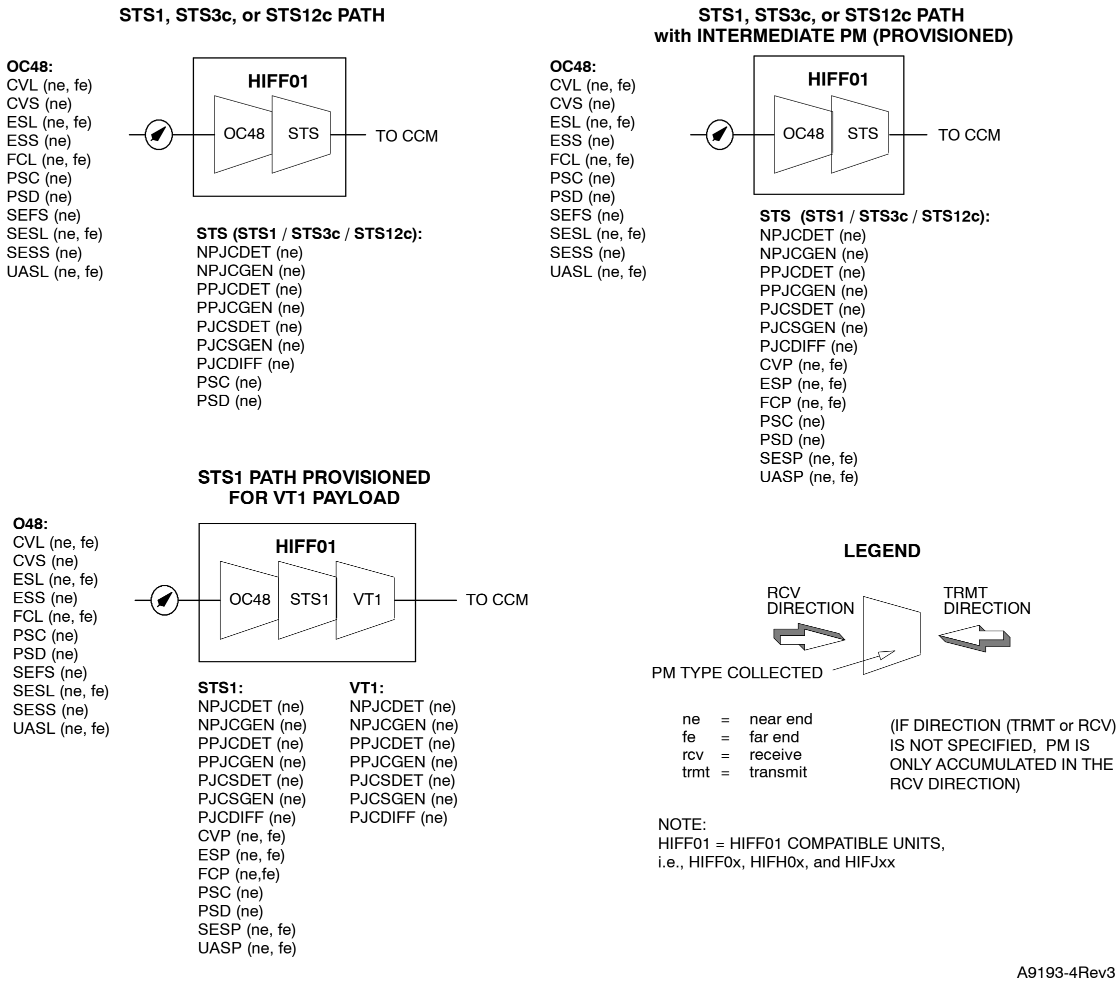


Figure 3. Performance Monitoring (PM) of OC48 Equipped Line Groups

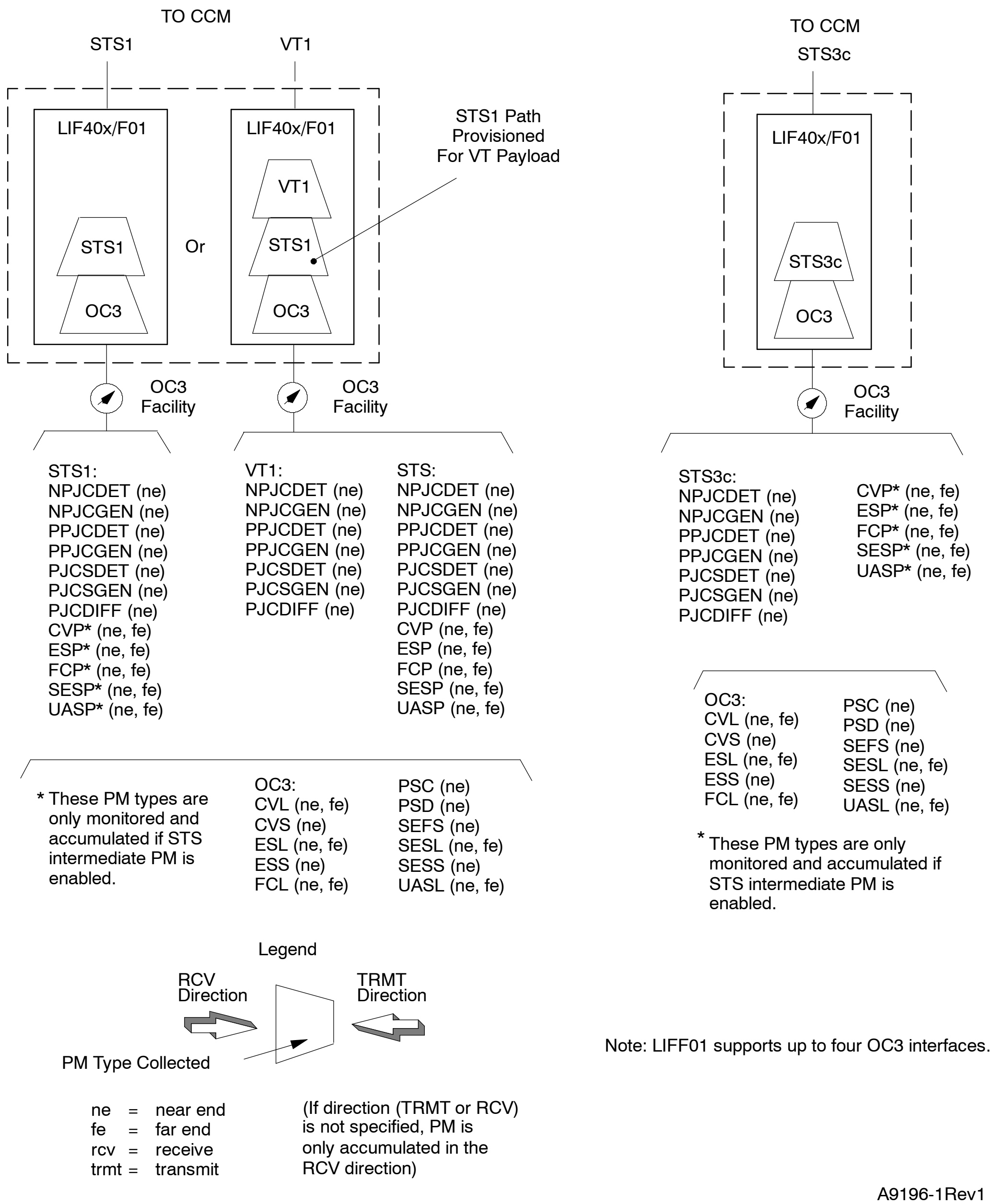


Figure 4. Performance Monitoring (PM) of OC3 Equipped Drop Groups

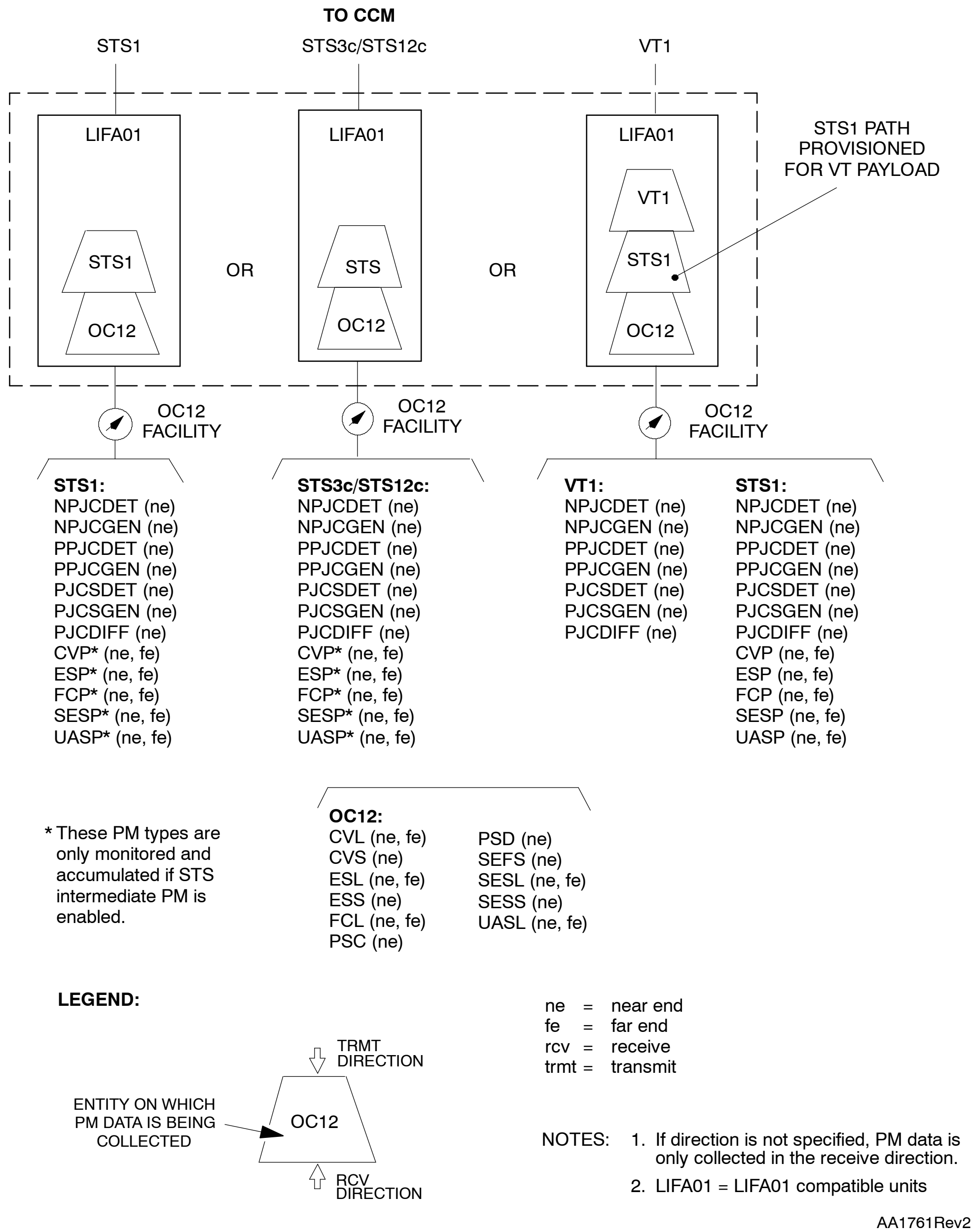


Figure 5. Performance Monitoring (PM) of OC12 Equipped Drop Groups

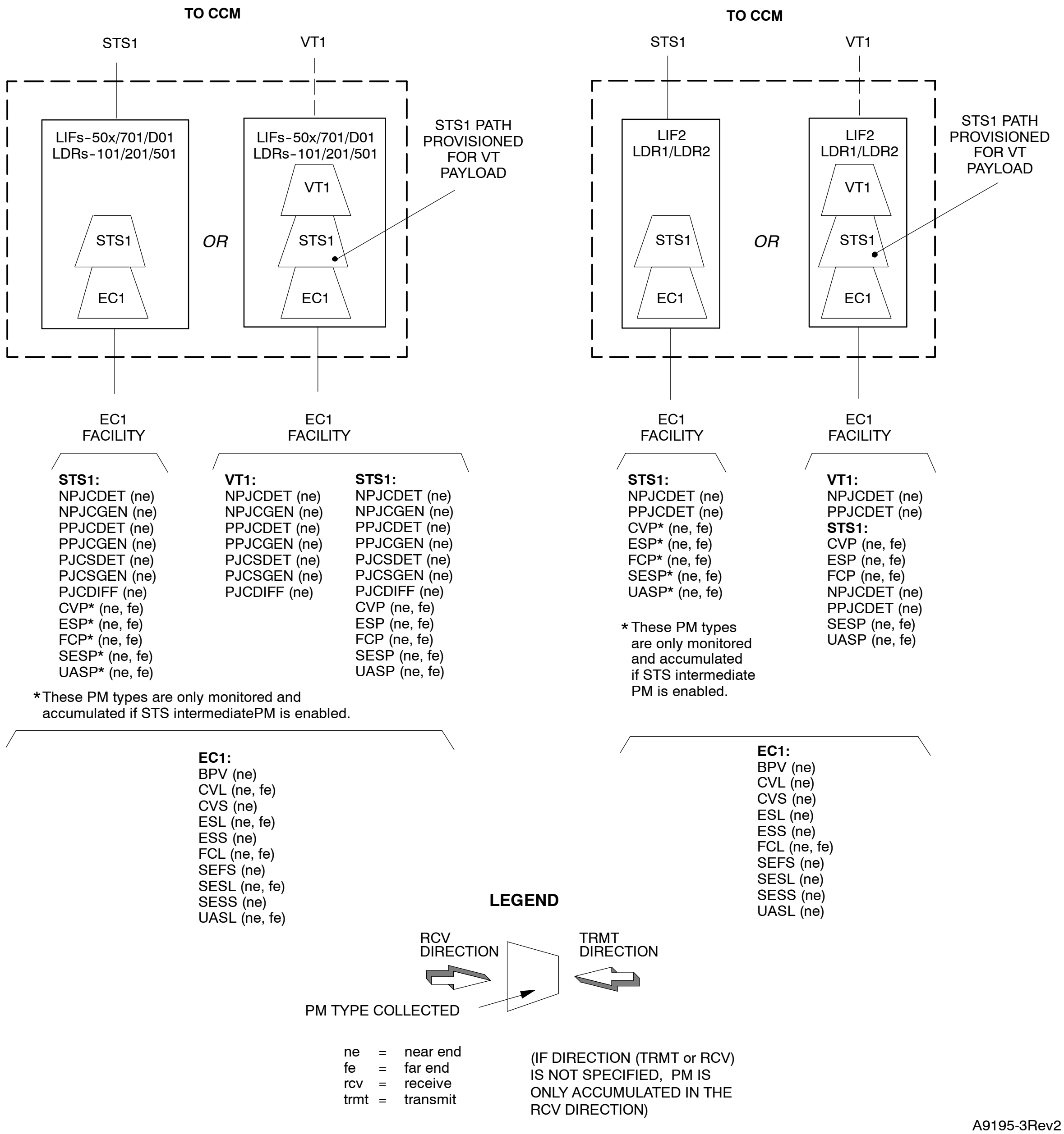


Figure 6. Performance Monitoring (PM) of EC1 Equipped Drop Groups

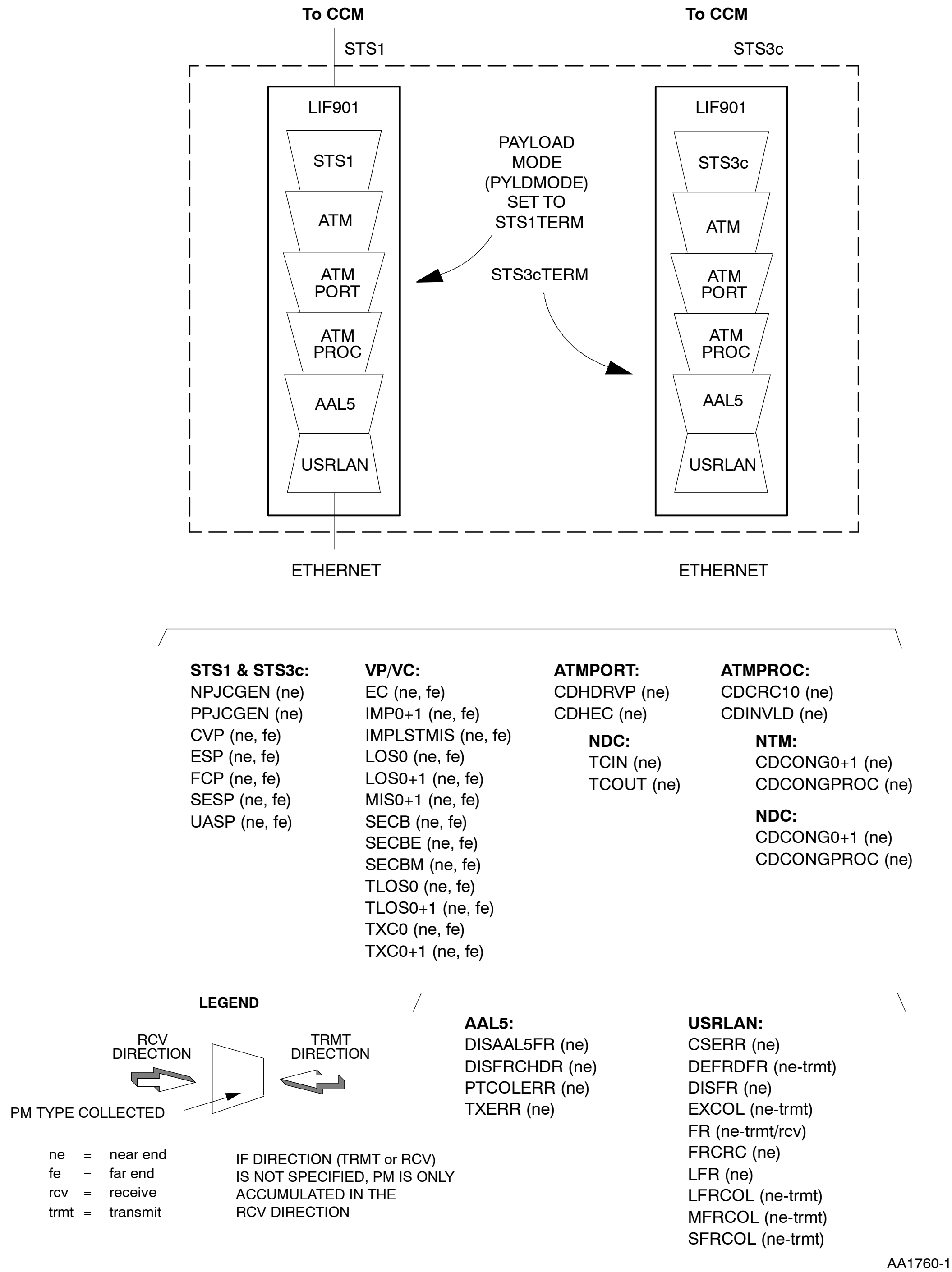


Figure 7. Performance Monitoring (PM) of USRLAN Drop Groups (LIF901)

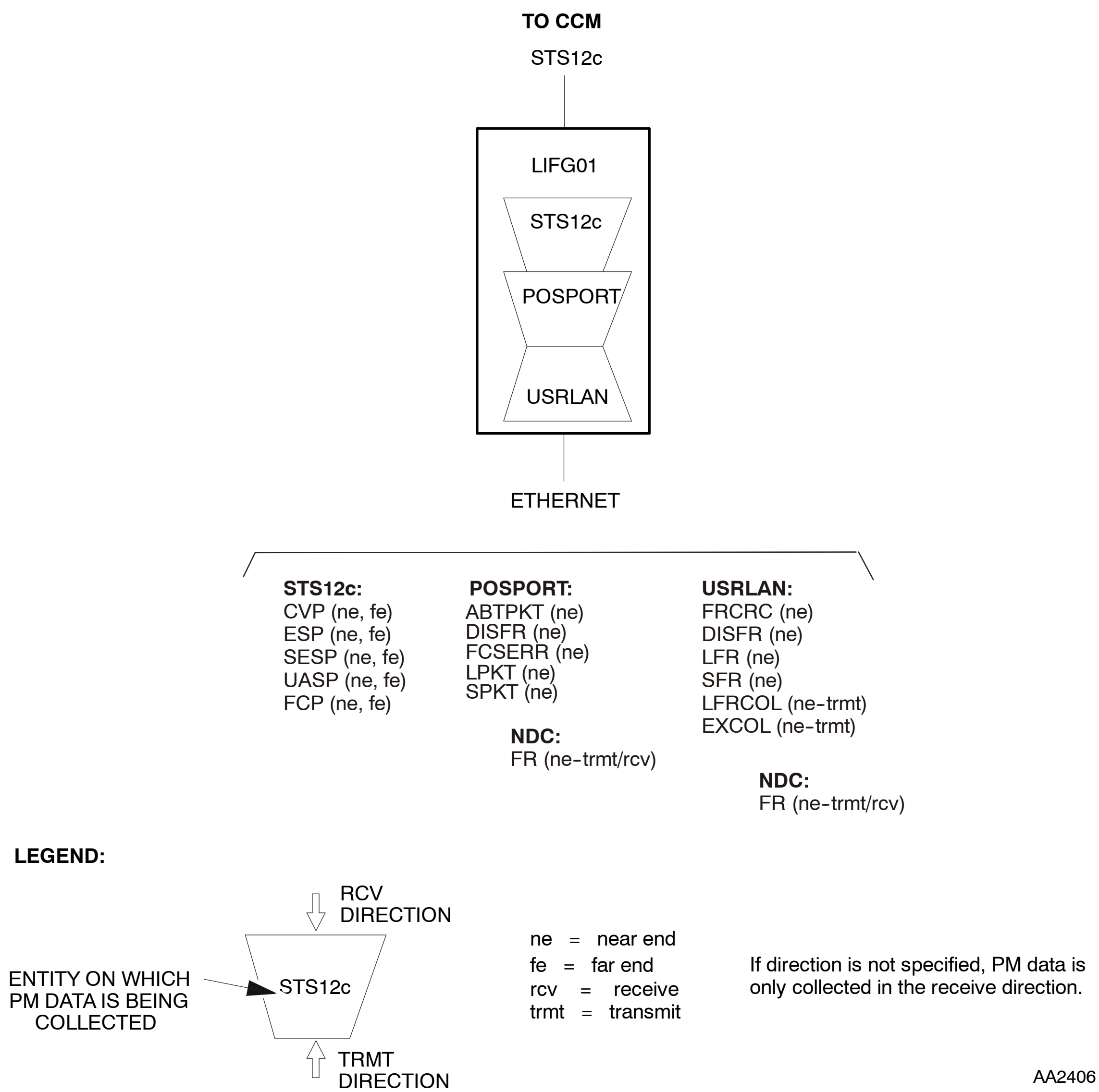


Figure 8. Performance Monitoring (PM) of USRLAN Drop Groups (LIFG01)

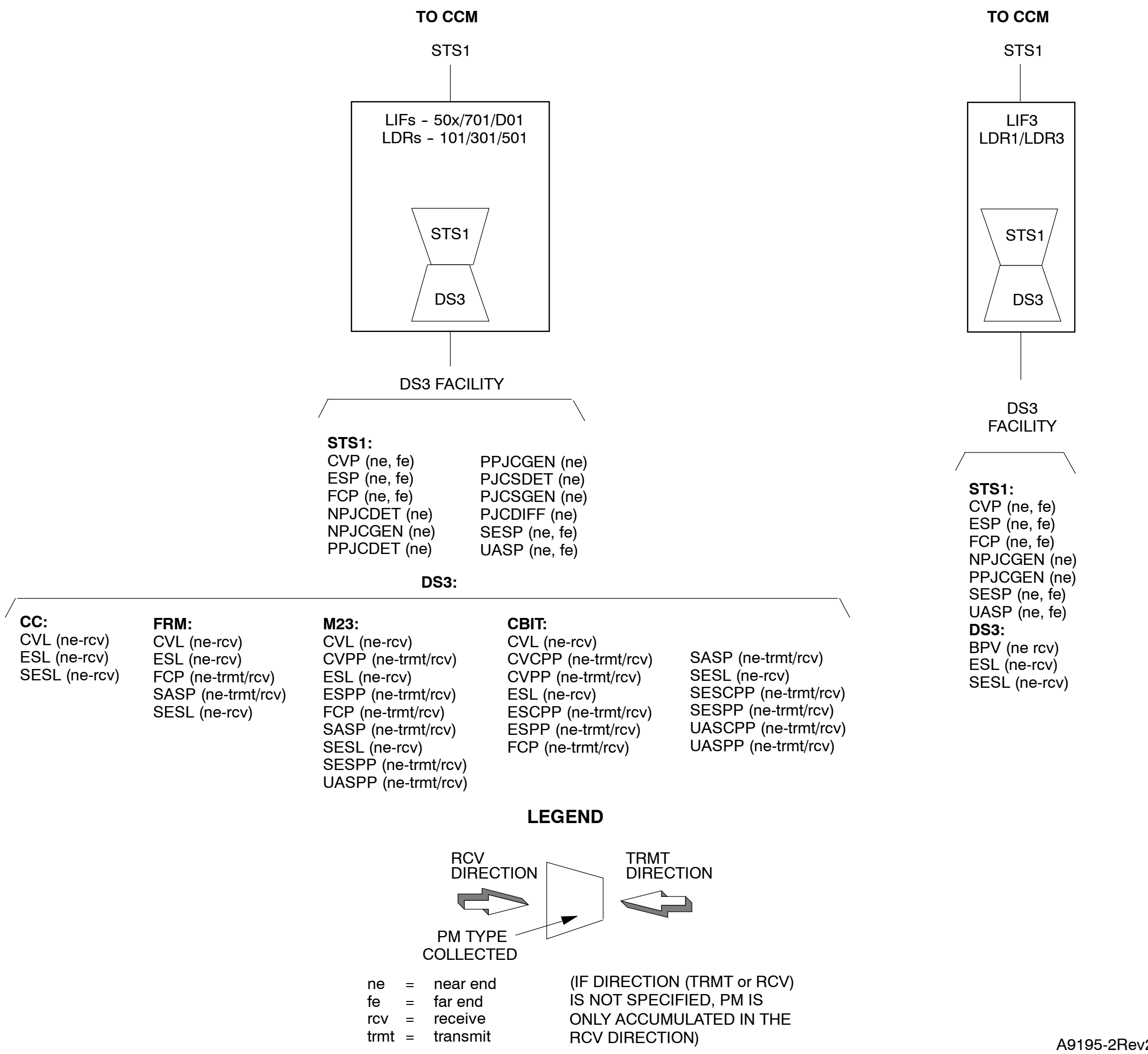


Figure 9. Performance Monitoring (PM) of DS3 Equipped Drop Groups

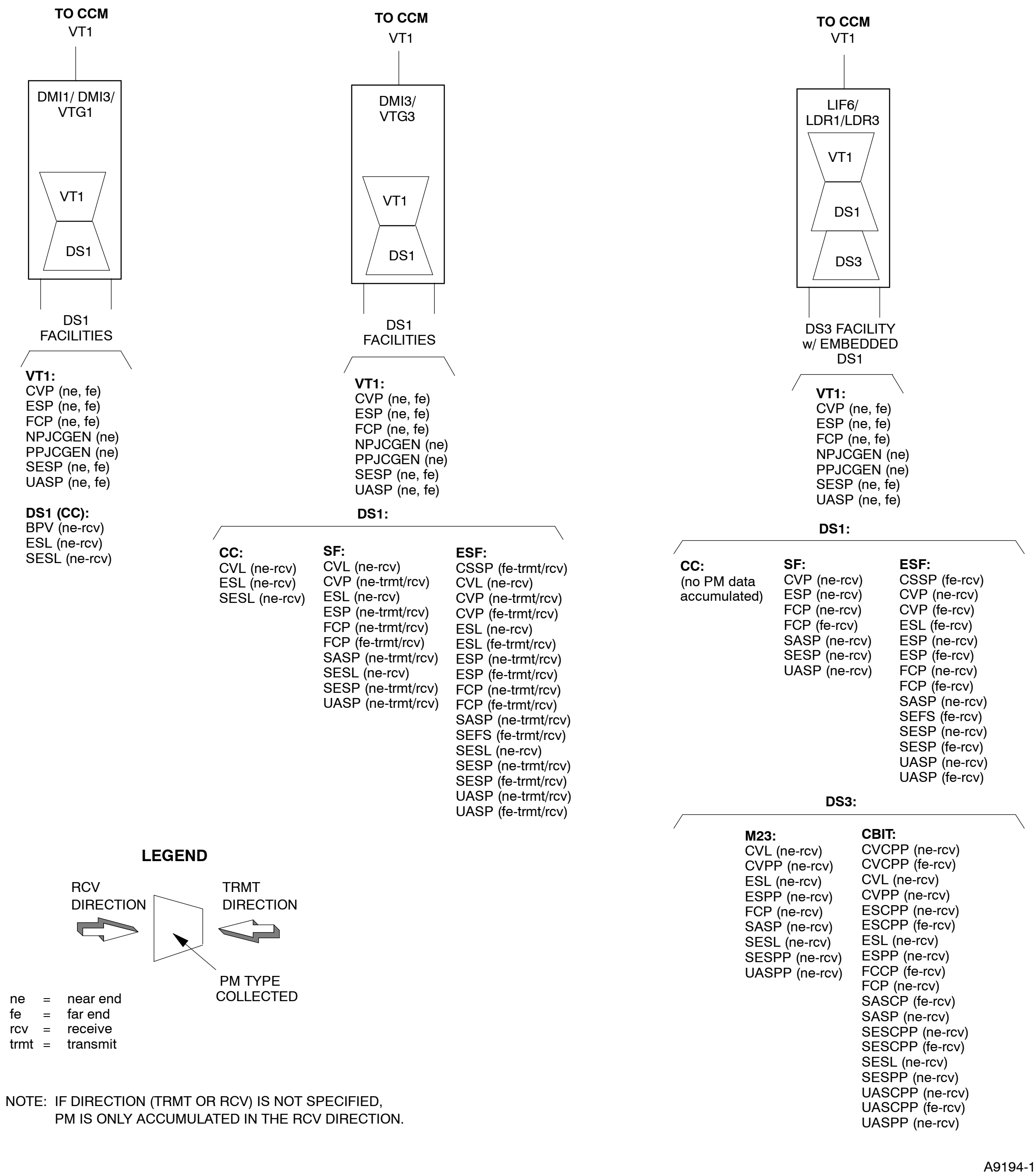


Figure 10. Performance Monitoring (PM) of DS1 and DS3/DS1 Transmux Equipped Drop Groups

STEP	PROCEDURE
1	Find the performance monitoring task to be performed in Table A and go to the step indicated.

Table A. Performance Monitoring Tasks

TASK	STEP
Equipment Performance Monitoring Tasks (LIF, LDR, DMI, VTG, CLK, CCM)	
Retrieve Equipment PM Information	2
Initialize (Set to Zero) Equipment PM Registers	4
Facility Performance Monitoring Tasks (OC3, OC12, EC1, DS3,USRLAN, AAL5, etc.)	
Retrieve Facility PM Information	6
Initialize (Set to Zero) Facility PM Registers	8
Retrieve Facility PM Threshold Levels	10
Change Facility PM Threshold Levels	12
Path Performance Monitoring Tasks (STS1, STS3c, VT1.5, VCL, etc.)	
Retrieve Path PM Information	15
Initialize (Set to Zero) Path PM Registers	17
Retrieve Path PM Threshold Levels	19
Change Path PM Threshold Levels	21
ATM Port Performance Monitoring Tasks	
Retrieve ATM Port PM Information	24
Initialize (Set to Zero) ATM Port PM Registers	26
Retrieve ATM Port PM Threshold Levels	28
Change ATM Port PM Threshold Levels	30
ATM Processor Performance Monitoring Tasks	
Retrieve ATM Processor PM Information	32
Initialize (Set to Zero) ATM Processor PM Registers	34
Retrieve ATM Processor PM Threshold Levels	36
Change ATM Processor PM Threshold Levels	37
POS Port Performance Monitoring Tasks	
Retrieve POS Port PM Information	39
Initialize (Set to Zero) POS Port PM Registers	41
Retrieve POS Port PM Threshold Levels	43
Change POS Port PM Threshold Levels	45

Table A. Performance Monitoring Tasks (cont)

TASK	STEP
Synchronization Performance Monitoring Tasks	
Retrieve Synchronization PM Data	47
Initialize (Set to Zero) Synchronization Registers	49
Performance Monitoring Mode Tasks (Equipment, Facilities, Paths, etc.)	
Retrieve PM Mode Information	51
Change PM Mode	53

Retrieve Equipment PM Information

2 Perform the following steps to retrieve current PM information for LIF, LDR, DMI, VTG, CLK, and/or CCM:

a. In the scope pane, expand Equipment and select equipment type for which PM data is being retrieved.

b. In the result pane, right-click unit for which PM data is being retrieved.

c. From the context menu, select **Task>Monitor>Performance** to open a work view.

d. On the work view, note PM data; then close work view.

3 STOP. This procedure is complete.

Initialize (Set to Zero) Equipment PM Registers

4 Perform the following steps to initialize equipment PM registers for LIF, LDR, DMI, VTG, CLK, and/or CCM:

a. In the scope pane, expand Equipment and select equipment type.

b. In the result pane, right-click unit on which PM registers are being initialized.

c. From the context menu, select **Task>Monitor>Performance** to open a work view.

d. On the toolbar, select Clear; then close work view.

5 STOP. This procedure is complete.

Retrieve Facility PM Information

6 Perform the following steps to retrieve facility PM information:

a. In the scope pane, expand Facility and select type of facility for which PM data is being retrieved.

b. In the result pane, right-click facility for which PM data is being retrieved.

c. From the context menu, select **Task>Monitor>Performance** to open a work view.

d. On work view, note current value in PM registers; then close work view.

NOTE: *The 1301 NMX retrieves register values specified by the number of seconds shown in the Refresh Rate field.*

7 STOP. This procedure is complete.

Initialize (Set to Zero) Facility PM Registers

8 Perform the following steps to initialize facility PM registers:

a. In the scope pane, expand Facility and select type of facility on which PM registers are being initialized.

b. In the result pane, right-click facility on which PM registers are being initialized.

c. From the context menu, select **Task>Monitor>Performance** to open a work view.

d. On the toolbar select Clear. then close work view.

NOTE: *The 1301 NMX retrieves register values specified by the number of seconds shown in the Refresh Rate field.*

9 STOP. This procedure is complete.

Retrieve Facility PM Threshold Levels

10 Perform the following steps to retrieve facility threshold levels:

a. In the scope pane, expand Facility and select type of facility for which PM threshold levels are being retrieved.

b. In the result pane, right-click facility for which PM threshold levels are being retrieved.

c. From the context menu, select **Task>Provision>PM Threshold** to open a work view.

d. On work view, note PM threshold levels; then close work view.

11 STOP. This procedure is complete.

Change Facility PM Threshold Levels

12 If a threshold level is changed to its default value, obtain the initial default threshold value for the facility from one of the following tables:

For OC48, refer to Table B.
For OC12, refer to Table C.
For OC3, refer to Table D.
For DS3, refer to Table E.
For EC1, refer to Table F.
For DS1, refer to Table G.
For USRLAN, refer to Table H.
For AAL5, refer to Table I.

13 Perform the following steps to change a facility threshold level:

a. In the scope pane, expand Facility and select type of facility on which PM threshold level is being changed (e.g., OC12, OC3, EC1, etc.).

b. In the result pane, right-click facility on which PM threshold level is being changed.

c. From the context menu that is displayed, select **Task>Provision>PM Threshold** to open a work view.

d. Find the error condition to change and use the spin-box in the 15-minute or 1-day value column to change the value.

e. On the toolbar, select Submit icon; then close work view.

14 STOP. This procedure is complete.

Table B. OC48 PM Threshold Levels

MONITOR TYPE	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERL-HT	4		3...5	Bit Error Ratio Line – High Threshold (SFBER)
BERL-LT	7		5...9	Bit Error Ratio Line – Low Threshold (DGBER)
CVL	21260	212602	1...4,294,967,295	Line Coding Violations
CVS	21499	214991	1...4,294,967,295	Coding Violation count – Section
DSESL	40300		1...65535	Number of coding violations to make one SESL
DSESS	23100		1...65535	Number of coding violations to make one SESS
ESL	180	1800	1...65535	Line Errored Seconds
ESS	180	1800	1...65535	Section Errored Seconds
SEFS	2	17	1...65535	Severely Errored Framing Seconds – OOFS/COFAS
SESL	3	7	1...65535	Line Severely Errored Seconds
SESS	3	7	1...65535	Section Severely Errored Seconds
UASL	10	10	1...65535	Line Unavailable Seconds

Table C. OC12 PM Threshold Levels

MONITOR	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERL-HT	4		3...5	Bit Error Ratio Line – High Threshold (SFBER)
BERL-LT	7		5...9	Bit Error Ratio Line – Low Threshold (DGBER)
CVL	5315	53150	1...4,294,967,295	Coding Violation count – Line
CVS	5375	53748	1...4,294,967,295	Coding Violation count – Section
DSESL	10000		1...65535	Number of coding violations to make one SESL
DSESS	8800		1...65535	Number of coding violations to make one SESS
ESL	60	600	1...65535	Line Errored Seconds
ESS	60	600	1...65535	Section Errored Seconds
SEFS	2	17	1...65535	Severely Errored Framing Seconds – OOFS/COFAS
SESL	3	7	1...65535	Line Severely Errored Seconds
SESS	3	7	1...65535	Section Severely Errored Seconds
UASL	10	10	1...65535	Line Unavailable Seconds

Table D. OC3 PM Threshold Levels

MONITOR TYPE	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERL-HT	4		3...5	Bit Error Ratio Line – High Threshold (SFBER)
BERL-LT	7		5...9	Bit Error Ratio Line – Low Threshold (DGBER)
CVL	1328	13288	1...4,294,967,295	Coding Violation count – Line
CVS	1344	13437	1...4,294,967,295	Coding Violation count – Section
DSESL	2500		1...65535	Number of coding violations to make one SESL
DSESS	2500		1...65535	Number of coding violations to make one SESS
ESL	20	200	1...65535	Line Errored Seconds
ESS	20	200	1...65535	Section Errored Seconds
SEFS	2	17	1...65535	Severely Errored Framing Seconds – OOFS/COFAS
SESL	3	7	1...65535	Line Severely Errored Seconds
SESS	3	7	1...65535	Section Severely Errored Seconds
UASL	10	10	1...65535	Line Unavailable Seconds

Table E. DS3 PM Threshold Levels

MONITOR TYPE	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERL-HT	4		4...9	Bit Error Ratio Line — High Threshold (SFBER)
BPV	387	3865	1...4,294,967,295	Bipolar violations
CVCPP	382	3820	1...4,294,967,295	CP-bit Errors
CVL	387	3865	1...4,294,967,295	Line Coding Errors
CVPP	382	3820	1...4,294,967,295	P-bit Errors
DSESCPP	44		1...65535	SESCPP Coding Violations
DSESL	44		1...65535	Number of coding violations to make one SESL
DSESPP	44		1...65535	SESPP Coding Violations
ESCPP	25	250	1...65535	CP-bit Path Errored Seconds
ESL	25	250	1...65535	Line Errored Seconds
ESPP	25	250	1...65535	P-bit Path Errored Seconds
SASP	2	8	1...65535	SEF/AIS Seconds
SASCP	2	8	1...65535	SEF/AIS (X-Bits)
SESCPP	4	40	1...65535	CP-bit Path SES
SESL	4	40	1...65535	Line Severely Errored Seconds
SESPP	4	40	1...65535	P-bit Path SES
UASCPP	10	10	1...65535	CP-bit Path Unavailable Seconds
UASPP	10	10	1...65535	P-bit Path Unavailable Seconds

Table F. EC1 PM Threshold Levels

MONITOR TYPE	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERL-HT	4		3…4	Bit Error Ratio Line – High Threshold (SFBER)
BERL-LT	7		5…9	Bit Error Ratio Line – Low Threshold (DGBER)
BPV	443	4428	1…4,294,967,295	Bipolar Violations
CVL	443	4428	1…4,294,967,295	Coding Violation count – Line
CVS	448	4470	1…4,294,967,295	Coding Violation count – Section
DSESL	2500		1…65535	Number of coding violations to make one SESL
DSESS	2500		1…65535	Number of coding violations to make one SESS
ESL	12	100	1…65535	Line Errored Seconds
ESS	12	100	1…65535	Section Errored Seconds
SEFS	2	17	1…65535	Severely Errored Framing Seconds – OOFS/COFAS
SESL	3	7	1…65535	Line Severely Errored Seconds
SESS	3	7	1…65535	Section Severely Errored Seconds
UASL	10	10	1…65535	Line Unavailable Seconds

Table G. DS1 PM Threshold Levels

MONITOR TYPE	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERL-HT	4		3...6	Bit Error Ratio Line – High threshold (SFBER)
BPV	13340	133400	1...4,294,967,295	Bipolar violations
CSSP	1	4	1...65535	Path Controlled slip seconds
CVL	13340	133400	1...4,294,967,295	Coding violation count – Line
CVP (FMT=SF)	72	691	1...4,294,967,295	Coding violation count – Path
CVP (FMT=ESF)	13296	132960		
ESL	65	648	1...65535	Line Errored Seconds
ESP	65	648	1...65535	Path Errored Seconds
SASP	2	17	1...65535	Path AIS seconds
SEFS	2	17	1...65535	Severely errored framing seconds (OOFS/COFAS)
SESL	10	100	1...65535	Line Severely Errored Seconds
SESP	10	100	1...65535	Path Severely Errored Seconds
UASP	10	10	1...65535	Unavailable seconds – Path

Table H. USRLAN PM Threshold Levels

MONITOR TYPE	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
CSERR[1]	24	2304	1...4,294,967,295	Number of Carrier Sense Errors
DISFR	40	3840	1...4,294,967,295	Number of received frames discarded due to no buffer available
EXCOL	24	2304	1...4,294,967,295	Excessive Collisions
FRCRC	4	384	1...4,294,967,295	Number of received frames with bad FCS (CRC errors)
LFR	8	768	1...4,294,967,295	Number of received frames longer than the maximum length
LFRCOL	24	2304	1...4,294,967,295	Multiple collision frames
SFR[2]	8	768	1...4,294,967,295	Number of received frames shorter than the minimum length

[1] Only pertains to LIF901
[2] Only pertains to LIFG01

Table I. AAL5 PM Threshold Levels

MONITOR TYPE	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
DISAAL5FR	12	48	1...4,294,967,295	Number of AAL5 frames discarded due to no buffer space
DISRFCHDR	4	18	1...4,294,967,295	Number of AAL5 frames discarded due to bad RFC-1483 header
PTCOLERR	3	288	1...4,294,967,295	Sum of protocol errors
TXERR	2	192	1...4,294,967,295	Sum of transfer errors

Retrieve Path PM Information

15 Perform the following steps to retrieve path PM information:

a. In the scope pane, expand Facility; then expand the facility type that contains the path for which PM information is to be received and select the path type.

b. In the result pane, right-click path for which PM information is being retrieved.

c. From the context menu that is displayed, select **Task>Monitor>Performance** to open a work view.

d. On the work view, note values in path PM registers; then close work view.

16 STOP. This procedure is complete.

Initialize (Set to Zero) Path PM Registers

17 Perform the following steps to initialize path PM registers:

a. In the scope pane, expand Facility; then expand the facility type that contains the path on which path PM registers are to be initialized and select the path type.

b. In the result pane, right-click path on which you want to initialize PM registers.

c. From the context menu that is displayed, select **Task>Monitor>Performance** to open a work view.

d. On the toolbar select Clear icon; then close work view.

18 STOP. This procedure is complete.

Retrieve Path PM Threshold Levels

19 Perform the following steps to retrieve path threshold levels:

a. In the scope pane, expand Facility; then expand the facility that contains the path for which path PM threshold levels are to be retrieved and select the path.

b. In the result pane, right-click path on which PM threshold level is being retrieved.

c. From the context menu, select **Task>Provision>PM Threshold** to open a work view.

d. On work view, note PM threshold levels; then close work view.

20 STOP. This procedure is complete.

Change Path PM Threshold Levels

21 If threshold levels are changing to their default values, obtain the initial default threshold levels for the path.

For an STS12c path, refer to Table J.
For an STS3c path, refer to Table K.
For an STS1 path, refer to Table L.
For a VT1 path, refer to Table M.
For a VCL/VPL, refer to Table N.

22 Perform the following steps to change a path threshold level:

a. In the scope pane, expand Facility; then expand the facility type that contains the path on which path PM threshold is to be changed, and select the path type.

b. In the result pane, right-click path on which PM threshold level is being changed.

c. From the context menu that is displayed, select **Task>Provision>PM Threshold** to open a work view.

d. Find the error condition to change and use the spin-box in the 15-minute or 1-day value column to change the value.

e. On the toolbar, select Submit icon; then close work view.

23 STOP. This procedure is complete.

Table J. STS12c PM Threshold Levels

MONITOR TYPE	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERP-HT	4		4	Bit Error Ratio – High Threshold (SFBER)
BERP-LT	6		5...9	Bit Error Ratio – Low Threshold (DGBER)
CVP	75	750	1...4,294,967,295	Coding Violation count – Path (near end or far end)
DSESP	8600		1...65535	Number of coding violations to make one SESP (one threshold used by both near end or far end counts)
ESP	60	600	1...65535	STS Path Errored Seconds (near end or far end)
NPJCDET	60	5760	1...4,294,967,295	Negative Pointer Justification Count Detected
NPJCGEN	60	5760	1...4,294,967,295	Negative Pointer Justification Count Generated
PPJCDET	60	5760	1...4,294,967,295	Positive Pointer Justification Count Detected
PPJCGEN	60	5760	1...4,294,967,295	Positive Pointer Justification Count Generated
PJCSDET	60	5760	1...65535	Pointer Justification Count Seconds Detected
PJCSGEN	60	5760	1...65535	Pointer Justification Count Seconds Generated
PJCDIFF	60	5760	1...4,294,967,295	Pointer Justification Count Difference
SESP	3	7	1...65535	STS Path Severely Errored Seconds (near end or far end)
UASP	10	10	1...65535	STS Path Unavailable Seconds (near end or far end)

Table K. STS3c PM Threshold Levels

MONITOR TYPE	DEFAULT 15-MIN	DEFAULT 1-DAY	RANGE	DESCRIPTION
BERP-HT	4		4	Bit Error Ratio Path – High Threshold (SFBER)
BERP-LT	6		5...9	Bit Error Ratio Path – Low Threshold (DGBER)
CVP *	25	250	1...4,294,967,295	Coding Violation count – Path (near end or far end)
DSESP	2400		1...65535	Number of coding violations to make one SESP (one threshold used by both near end or far end counts)
ESP	20	200	1...65535	STS Path Errored Seconds (near end or far end)
NPJCDET	60	5760	1...4,294,967,295	Negative Pointer Justification Count Detected
NPJCGEN	60	5760	1...4,294,967,295	Negative Pointer Justification Count Generated
PPJCDET	60	5760	1...4,294,967,295	Positive Pointer Justification Count Detected
PPJCGEN	60	5760	1...4,294,967,295	Positive Pointer Justification Count Generated
PJCSDET	60	5760	1...65535	Pointer Justification Count Seconds Detected
PJCSGEN	60	5760	1...65535	Pointer Justification Count Seconds Generated
PJCDIFF	60	5760	1...4,294,967,295	Pointer Justification Count Difference
SESP	3	7	1...65535	STS Path Severely Errored Seconds (near end or far end)
UASP	10	10	1...65535	STS Path Unavailable Seconds (near end or far end)

* *Default values for an STS3c path that terminates on an LIF901 are 15 (15-MIN) and 125 (1-DAY).*

Table L. STS1 PM Threshold Levels

MONITOR TYPE	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERP-HT	4		3...4	Bit Error Ratio – High Threshold (SFBER)
BERP-LT	6		5...9	Bit Error Ratio – Low Threshold (DGBER)
CVP	15	125	1...4,294,967,295	Coding Violation count – Path (near end or far end)
DSESP	2400		1...65535	Number of coding violations to make one SESP (one threshold used by both near end or far end counts)
ESP	12	100	1...65535	STS Path Errored Seconds (near end or far end)
NPJCDET	60	5760	1...4,294,967,295	Negative Pointer Justification Count Detected
NPJCGEN	60	5760	1...4,294,967,295	Negative Pointer Justification Count Generated
PPJCDET	60	5760	1...4,294,967,295	Positive Pointer Justification Count Detected
PPJCGEN	60	5760	1...4,294,967,295	Positive Pointer Justification Count Generated
PJCSDET	60	5760	1...65535	Pointer Justification Count Seconds Detected
PJCSGEN	60	5760	1...65535	Pointer Justification Count Seconds Generated
PJCDIFF	60	5760	1...4,294,967,295	Pointer Justification Count Difference
SESP	3	7	1...65535	STS Path Severely Errored Seconds (near end or far end)
UASP	10	10	1...65535	STS Path Unavailable Seconds (near end or far end)

Table M. VT1 PM Threshold Levels

MONITOR TYPE	DEFUALT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERP-HT	4		3...4	Bit Error Ratio Path – High threshold (SFBER).
BERP-LT	6		5...8	Bit Error Ratio Path – Low threshold (DGBER)
CVP	15	146	1...4,294,967,295	Coding Violation count – Path (near end or far end)
DSESP	600		1...65535	Number of coding violations to make one SESP
ESP	12	117	1...65535	VT Path Errored Seconds (near end or far end)
NPJCDET	2	192	1...4,294,967,295	Negative Pointer Justification Count Detected
NPJCGEN*	2	192	1...4,294,967,295	Negative Pointer Justification Count Generated
PPJCDET	2	192	1...4,294,967,295	Positive Pointer Justification Count Detected
PPJCGEN*	2	192	1...4,294,967,295	Positive Pointer Justification Count Generated
PJCSDET	2	192	1...65535	Pointer Justification Count Seconds Detected
PJCSGEN	2	192	1...65535	Pointer Justification Count Seconds Generated
PJCDIFF	2	192	1...4,294,967,295	Pointer Justification Count Difference
SESP	3	7	1...65535	Path Severely Errored Seconds (near end or far end)
UASP	10	10	1...65535	Path Unavailable Seconds (near end or far end)

* *The range for LIF601 and DMI equipped drop groups is 1...65535.*

Table N. VCL/VPL PM Threshold Levels

MONITOR TYPE	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
IMP0+1	148	14208	1...4,294,967,295	Impaired cell blocks
SECB	125	12000	1...4,294,967,295	Severely Errored Cell Blocked
TLOS0	180	17280	1...4,294,967,295	Total lost 0 user information cells
TLOS0+1	220	21120	1...4,294,967,295	Total lost 0+1 user information cells

Retrieve ATM Port PM Information

24 Perform the following steps to retrieve ATM Port PM information:

a. In the scope pane, expand Facility; then expand USRLAN and select ATM Port.

b. In the result pane, right-click ATM Port for which PM information is being retrieved.

c. From the context menu that is displayed, select **Task>Monitor>Performance** to open a work view.

d. On the work view, note values in ATM Port PM registers; then close work view.

25 STOP. This procedure is complete.

Initialize (Set to Zero) ATM Port PM Registers

26 Perform the following steps to initialize port PM registers:

a. In the scope pane, expand Facility; then expand USRLAN and select ATM Port.

b. In the result pane, right-click ATM Port on which PM registers are being initialized.

c. From the context menu that is displayed, select **Task>Monitor>Performance** to open a work view.

d. On the toolbar, select Clear icon; then close work view.

27 STOP. This procedure is complete.

Retrieve ATM Port PM Threshold Levels

28 Perform the following steps to retrieve ATM Port threshold levels:

a. In the scope pane, expand Facility; then expand USRLAN and select ATM Port.

b. In the result pane, right-click ATM Port for which PM information is being retrieved.

c. From the context menu that is displayed, select **Task>Provision>PM Threshold** to open a work view.

d. On work view, note PM threshold levels; then close work view.

29 STOP. This procedure is complete.

Change ATM Port PM Threshold Levels

30 If PM threshold levels are being changed to their default values, obtain the initial default values from Table O.

a. In the scope pane, expand Facility; then expand USRLAN and select ATM Port.

b. In the result pane, right-click ATM Port on which PM threshold is being changed.

c. From the context menu that is displayed, select **Task>Provision>PM Threshold** to open a work view.

d. Find the error condition to change and use the spin-box in the 15-minute or 1-day value column to change the value.

e. On the toolbar, select Submit icon; then close work view.

31 STOP. This procedure is complete.

Table O. ATM Port PM Threshold Levels

MONITOR TYPE	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
CDHDRVP	20	1920	1...4,294,967,295	Cells discarded due to ATM layer header errors in VPI field
CDHEC	900	86400	1...4,294,967,295	Cells discarded due to HEC violations

Retrieve ATM Processor PM Information

32 Perform the following steps to retrieve ATM Processor PM information:

a. In the scope pane, expand Facility and select ATM Processor.

b. In the result pane, right-click ATM Processor for which PM information is being retrieved.

c. From the context menu that is displayed, select **Task>Monitor>Performance** to open a work view.

d. On work view, note values in ATM Processor PM registers; then close work view.

33 STOP. This procedure is complete.

Initialize (Set to Zero) ATM Processor PM Registers

34 Perform the following steps to initialize ATM Processor PM registers:

a. In the scope pane, expand Facility and select ATM Processor.

b. In the result pane, right-click ATM Processor on which PM registers are being initialized.

c. From the context menu that is displayed, select **Task>Monitor>Performance** to open a work view.

d. On the toolbar, select Clear icon; then close work view.

35 STOP. This procedure is complete.

Retrieve ATM Processor PM Threshold Levels

36 Perform the following steps to retrieve ATM Processor PM threshold levels:

a. In the scope pane, expand Facility and select ATM Processor.

b. In the result pane, right-click ATM Processor for which PM threshold level is being retrieved.

c. From the context menu that is displayed, select **Task>Provision>PM Threshold** to open a work view.

d. On work view, note PM threshold levels; then close work view.

Change ATM Processor PM Threshold Levels

37 If threshold levels are being charged to their default values, obtain the initial default threshold levels from Table P.

a. In the scope pane, expand Facility and select ATM Processor.

b. In the result pane, right-click ATM Processor on which PM threshold is being changed.

c. From the context menu that is displayed, select **Task>Provision>PM Threshold** to open a work view.

d. Find the monitor type to change and use the spin-box in the 15-minute or 1-day value column to change the value.

e. On the toolbar, select Submit icon; then close work view.

Table P. ATM Processor PM Threshold Levels

MONITOR TYPE	DEFAULT			RANGE	DESCRIPTION
	5-MIN	15-MIN	1-DAY		
CDCRC10	–	2	80	1...4,294,967,295	OAM cells discarded due to CRC-10 errors
CDINVLD	–	12	600	1...4,294,967,295	OAM cells discarded due to invalid data
CDCONG0+1 (NTM)	5	–	–	1...4,294,967,295	Priority 0 and 1 cells (CLP=0+1) discarded due to congestion
CDCONGPRO C (NTM)	2	–	–	1...4,294,967,295	OAM cells discarded due to congestion in OAM processing

38 STOP. This procedure is complete.

Retrieve POS Port PM Information

39 Perform the following steps to retrieve POS Port PM information:

a. In the scope pane, expand Facility; then expand USRLAN and select POS Port.

b. In the result pane, right-click POS Port for which PM information is being retrieved.

c. From the context menu that is displayed, select **Task>Monitor>Performance** to open a work view.

d. On the work view, note values in POS Port PM registers; then close work view.

40 STOP. This procedure is complete.

Table Q. POS Port PM Threshold Levels

MONITOR TYPE	DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
ABTPKT	20	1920	1...4,294,967,295	The number of received abort sequence packets
DISFR	40	3840	1...4,294,967,295	The number of frames being discarded because no buffer is available
FCSERR	20	1920	1...4,294,967,295	The number of HDLC frames received with bad frame check sequence
LPKT	20	1920	1...4,294,967,295	The number of packets received that are longer than maximum allowed length
SPKT	20	1920	1...4,294,967,295	The number of packets received that are shorter than minimum allowed length

Initialize (Set to Zero) POS Port PM Registers

41 Perform the following steps to initialize POS Port PM registers:

a. In the scope pane, expand Facility; then expand USRLAN and select POS Port.

b. In the result pane, right-click POS Port for which PM information is being initialized.

c. From the context menu, select **Task>Monitor>Performance** to open a work view.

d. On the work view, select the register(s) you want to clear.

e. On the toolbar, select Clear icon; then close work view.

42 STOP. This procedure is complete.

Retrieve POS Port PM Threshold Levels

43 Perform the following steps to retrieve POS Port PM threshold levels:

a. In the scope pane, expand Facility; then expand USRLAN and select POS Port.

b. In the result pane, right-click POS Port for which PM information is being retrieved.

c. From the context menu that is displayed, select **Task>Provision>PM Threshold** to open a work view.

d. On work view, note PM threshold levels; then close work view.

44 STOP. This procedure is complete.

Change POS Port PM Threshold Levels

45 If changing PM threshold levels to their default values, obtain the initial default values from Table Q.

a. In the scope pane, expand Facility; then expand USRLAN and select POS Port.

b. In the result pane, right-click POS Port on which PM threshold is being changed.

c. From the context menu that is displayed, select **Task>Provision>PM Threshold** to open a work view.

d. Find the condition to change in the Name column and use the spin-box in the 15-Minute or 1-Day Value column to change the value.

e. On the toolbar, select Submit icon; then close work view.

46 STOP. This procedure is complete.

Retrieve Synchronization PM Data

47 Perform the following steps to retrieve synchronization PM data:

a. In the scope pane, expand System; then expand Synchronization and select NE Sync.

b. In the result pane, right-click NE Sync to display a context menu.

c. From the context menu, select **Task>Monitor>Performance** to open a work view.

d. On work view, note PM data; then close work view.

48 STOP. This procedure is complete.

Initialize (Set to Zero) Synchronization Registers

49 Perform the following steps to initialize synchronization registers:

a. In the scope pane, expand System; then expand Synchronization and select NE Sync.

b. In the result pane, right-click NE Sync to display a context menu.

c. From the context menu, select **Task>Monitor>Performance** to open a work view.

d. On the toolbar, select Clear icon; then close work view.

50 STOP. This procedure is complete.

Retrieve PM Mode Information

51 Perform the following steps to retrieve PM mode information:

a. Refer to Table R for selections to make in scope pane.

b. In the result pane, right-click entity for which PM mode is being retrieved to display a context menu.

c. From the context menu, select **Task>Provision>PM Mode** to open a work view.

d. On work view, note PM mode information; then close work view.

52 STOP. This procedure is complete.

Table R. Scope Pane Selections for PM Mode

TO RETRIEVE PM MODE FOR...	IN SCOPE PANE EXPAND...	THEN EXPAND...	AND SELECT...
Equipment	Equipment	–	LIF, LDR, DMI, VTG, CCM, or CLK
Facilities	Facility	–	OC3, OC12, OC48, EC1, DS3, DS3/DS1 Tmux, or DS1
Paths	Facility	USRLAN	STS1, STS3c, STS12c, VCL, or VPL
USRLAN Facility, AAL5, VCL/VPL, ATM Port, or POS Port	Facility	USRLAN	Entity being retrieved (i.e., AAL5, POS Port, etc.)
ATM Processor	Facility	–	ATM Processor
NE Sync	Facility	Synchronization	NE Sync

Change PM Mode

53 Perform the following steps to change PM mode:

a. Refer to Table R for selections to make in scope pane.

b. In the result pane, right-click entity on which PM mode is being changed to display a context menu.

c. From the context menu, select **Task>Provision>PM Mode** to open a work view.

d. On the work view, select desired settings.

e. On the toolbar, select Submit icon; then close work view.

54 STOP. This procedure is complete.

TAD-001
Maintenance Philosophy

1. General

1.1 The 1603 SMX Add/Drop Multiplexer is a member of Alcatel's Synchronous Optical Network (SONET) family of products. The 1603 SMX is designed to support Optical Carrier Level 3 (OC3), Optical Carrier Level 12 (OC12), and Optical Carrier Level 48 (OC48) line interfaces. It also supports four independent low speed drop groups. To provide more efficient processing and better fault tolerance, the 1603 SMX incorporates a distributed processor design. The NEP (shelf controller), HIF (OC3, OC12, and OC48 interfaces), CCM (cross-connect), and DMI/LIF (drop group controller) plug-in units each have independent processor and memory circuitry that provides improved survivability. The design of the 1603 SMX allows for backup units for all traffic-carrying plug-ins. Therefore, the failure of one unit does not interrupt service if the backup redundant or protection unit is equipped.

1.2 Like all of the Alcatel SONET products, once installed in a traffic-carrying network, the 1603 SMX becomes a Network Element (NE) that permits access to, provisioning, interrogation, and communication with any other NE within the network. The 1603 SMX is a software-controlled and software-provisioned device that can be placed locally or remotely in performance monitoring and diagnostic modes.

1.3 The 1603 SMX continuously performs diagnostic routines and status polling to determine if operational faults exist relative to hardware, software, or traffic handling. Plug-in units are polled for equipped/unequipped/type status, as well as their In-Service/Out-of-Service (IS/OOS) state.

1.4 If a fault is detected, alarm messages are generated. Depending on the nature of the alarm (critical, major, minor), local (visual/audible) and remote alarms are also activated. Most alarm conditions are described adequately by the alarm message. More specific trouble isolation can be done using the plug-in unit front panel alarm lamps and diagnostic commands. Plug-in unit alarm/status lamps and related switches are listed in TAD-002.

2. System Database and Memory

2.1 The NEP and COA plug-in units contain memory that stores data about the system configuration. The design of 1603 SMX provides automatic backup of all important information by use of redundant plug-in configurations and nonvolatile memory. Still, improper plug-in removal or command entries could inadvertently destroy data. It is important to follow instructions in the system manuals when entering commands and/or removing plug-ins.

2.2 The NEP/COA combination provides the system provisioning database memory. The NEP and COA databases are mirror images of each other. The NEP database is referred to as the working database and is volatile. Therefore, when it is removed, its copy of the database is lost. The COA database is referred to as the primary backup database. The COA database is nonvolatile and is maintained when removed or replaced. Under normal conditions, any changes in system status that affect the database are automatically made to both the working and primary databases.

2.3 The NEP/COA units store provisioning, performance threshold settings, and alarm reporting attributes information. The NEP also retains provisioning for the rest of the system, synchronization settings, security data, and communications settings. All of this is backed up on the COA. Performance monitoring data is not backed up on the COA. Various cards throughout the system collect performance monitoring data at various time increments. If these cards are pulled, or they fail, all of this accumulated reporting is lost. However, the performance threshold settings are safe. Message and data logs for system and security audit are also stored on the NEP, but are not backed up on the COA.

2.4 The COA has factory-default provisioning data that is provided when the unit is plugged into the system for the first time. The general default configuration is all equipment (except the COA, NEP, CLK, and PWR units), overhead channels and facilities are out-of-service and unassigned. The COA, NEP, CLK-A, CLK-B, PWR-A, PWR-B, and PWR-C plug-ins are assigned and in service since they are required in the minimum configuration. Also, the Craft 1 port on the COA is out-of-service, but assigned (OOS-MA-AS), which allows for communication with the system in the default state.

2.5 When replacing the COA, certain alarms may be raised, depending on which database (if any) is on the replacement COA. So the following assumptions are in order:

- If the replacement COA has been provisioned with a database that differs from the database on the NEP, a MEMDIF alarm is raised. The database can be copied from either unit to the other (using the CPY-MEM command) depending on which unit has the preferred database.

- If the replacement COA has a different database version (i.e., the COA had been removed from a system with a previous software release), a MEMVER alarm is raised. In this case, the database must be copied from the NEP to the COA.

- If the replacement COA has a blank database (new unit), the database is automatically copied from the NEP.

- If the COA is removed, and for some reason the NEP database is erased (power removed, NEP unplugged or reinitialized), the COA database is automatically copied to the NEP when installed.
- If the NEP is removed or replaced, the database is automatically copied from the COA to the NEP when plugged in.
- If the COA and NEP are both removed or replaced, the database present on the COA is copied to the NEP when plugged in.
- After successfully downloading the NEP with new software (during an in-service upgrade, for instance), a MEMDIFTRAN alarm is raised. This alarm indicates that any new provisioning data will be entered in the NEP memory but not the COA. This state allows reversion to the previous software release if any upgrade problems are encountered. The alarm is cleared by the CPY-MEM command.

2.6 The only danger of losing the database is if the database on the NEP is inadvertently erased while a faulty COA is being replaced.

3. Craft Interface

3.1 The local craft interface is provided through the Craft, Orderwire and Alarm (COA) front panel RS-232 port. On odd numbered COA units (COA601, 603, 605, etc.), a remote access RS-232 port (Craft 2) is also provided through the wire-wrap pins on the shelf backplane. Through either of these craft ports, maintenance personnel can command various tests to locate and confirm faults. Traffic reports are also available to aid in trouble analysis. Refer to TNG-503 for a description of the craft interface operation.

4. Trouble Analysis Procedures (TAPS)

4.1 Trouble Analysis Procedures (TAPs) for the 1603 SMX are provided in this document. TAPs generally assume the following:

- An alarm message has been received at the local NE (where the alarm originated), at a remote NE (CAMR concentrator), or at Operations System alarm monitoring equipment (through X.25 packet switched network or TBOS Serial E2A interface).
- Only one case of trouble exists even though several alarm conditions may be reported.
- Maintenance personnel are familiar with the 1603 SMX.
- Personnel are familiar with the 1301 NMX interface used to interact with the 1603 SMX system.

4.2 Trouble clearing begins with an analysis of the alarm message and/or other alarm indications. The applicable TAP is accessed through the Task Index List (IXL-001).

4.3 In the case of multiple alarms, alarms should be cleared in the following order:

1. Power (COM PWRF-48V) and Fuse (COM FA) alarms
2. Equipment (plug-in) alarms
3. USRLAN alarms
4. Traffic-carrying facility alarms (EC1, OC3, OC12, OC48, T1, T3)
5. SYNCN (synchronization) alarms
6. STS1/STS3c/STS12c path alarms
7. VT1 path alarms
8. ATM Port alarms
9. POS Port alarms
10. POS Port alarms
11. AAL5 alarms
12. ATM Processing Element alarms
13. VPL alarms
14. VCL alarms
15. All others

4.4 The basic maintenance philosophy for the 1603 SMX is to locate and replace failed units with a minimum of service interruption. Failed units should be returned to the manufacturer for repair and return. Provisioning data pertaining to replaced units is maintained and is not required to be reentered.

4.5 Care should be exercised when removing units, performing commands, etc., to avoid unnecessary service interruption. Since the NEP and COA house the system provisioning memory, these units should never be removed simultaneously.

4.6 When the replacement of a unit does not clear the trouble, the replacement unit should be removed and the original unit returned to service.

5. Conclusion

5.1 When the corrective action described in a TAP fails to clear the fault, an obscure or multiple fault is assumed to exist. For help in clearing this type of fault, contact Alcatel Customer Service.

TAD-002
Plug-in Unit Status Indicators/Switches

1. Plug-In Unit Status Indicators/Switches

1.1 Refer to Table A for plug-in unit status indicators/switches.

Table A. Plug-in Unit Status Indicators/Switches

UNIT	INDICATOR/ SWITCH	DESIGNATION	FUNCTION
CCMx01	LED, green	ACT	Indicates active/standby status of unit.
	LED, red	ALM	Indicates unit is in alarm.
CLK20x	LED, red	ALM	Indicates a failure on the CLK20x.
COAxxx	LED, red	CRI*	Indicates one or more alarms are active that have an assigned critical notification code (alarm attribute). The critical notification code is typically assigned to alarm conditions that are severely service-affecting and require immediate corrective action.
	LED, red	MAJ*	Indicates one or more alarms are active that have an assigned major notification code, which is typically assigned to alarm conditions that are service-affecting and require immediate corrective action, but urgency is less than a critical alarm because of a lesser number of lines affected.
	LED, yellow	MIN*	Indicates one or more alarms are active that have an assigned minor notification code, which is typically assigned to alarm conditions that are not service-affecting.

Table A. Plug-in Unit Status Indicators/Switches (cont)

UNIT	INDICATOR/ SWITCH	DESIGNATION	FUNCTION
COAxxx (cont)	LED, yellow	REM ALM	Indicates far-end alarm.
	LED, red	ALM	Indicates unit is in alarm.
	LED, green	ACO ACTIVE	Indicates alarm cut-off has been activated, but alarm may still exist.
	Switch	ACO/LAMP TEST	Silences current audible alarm and serves as a lamp test switch.
	Switch	NE ID ID SEL	Selects far-end NE identification.
	Seven-segment LED displays	1st, 2nd	Two-digit display that indicates the NE identification code of the remote alarm (REM ALM); selected by ID SEL switch.
DMIxxx	LED, green	ACT	Indicates unit is active.
	LED, red	ALM	Indicates unit is in alarm.
HIFxxx	LED, green	ACT	Indicates unit is active (carrying traffic).
	LED, yellow	SF	Indicates signal failure on facility.
	LED, red	ALM	Indicates unit is in alarm.
LDRxxx (except LDR501)	LED, green	ACT	Indicates unit is active (carrying traffic).
	LED, yellow	SF	Indicates signal failure on facility.
	LED, red	ALM	Indicates unit is in alarm.
LDR501	LED, green/yellow	PSA	Indicates protection status. LED is green when the protection unit is actively protecting another unit. LED is yellow when unit is actively being protected.
	LED, yellow	SF	Indicates signal failure on facility.
	LED, red	ALM	Indicates unit is in alarm.
LIF40x/A01	LED, green	ACT	Indicates unit is active.
	LED, red	ALM	Indicates unit is in alarm.
	LED, yellow	SF	Indicates signal failure on facility.
LIF901	LED, red	ALM	Indicates unit is in alarm.
	LED, yellow	SF -1, -2, -3, -4	Indicates ethernet port failure.

Table A. Plug-in Unit Status Indicators/Switches (cont)

UNIT	INDICATOR/ SWITCH	DESIGNATION	FUNCTION
LIFF01	LED, green	ACT	Indicates unit is active.
	LED, red	ALM	Indicates unit is in alarm.
	LED, yellow	SF -1, -2, -3, -4	Indicates signal failure on facility.
LIFG01	LED, red	ALM	Indicates unit failure.
	LED, yellow	SF	Indicates link status of Gigabit Ethernet interface
	LED, green	ACT	Indicates unit is active.
LIFxxx (All others)	LED, green	ACT	Indicates unit is active.
	LED, red	ALM	Indicates unit is in alarm.
NEPxxx	LED, green	ACT	Indicates unit is active controller of the system.
	LED, yellow	ABN	Indicates system is in abnormal state and requires operator attention.
	LED, red	ALM	Indicates unit is in alarm.
PWRA01	LED, green	ON	Indicates normal operation.
	LED, red	ALM	Indicates unit is OFF or that unit has failed but input voltage is applied.
VTG101	LED, yellow	SF	Indicates signal failure on facility.
	LED, red	ALM	Indicates unit is in alarm.
VTG102/ VTG30x	LED, yellow	SF	Indicates signal failure on facility.
	LED, red	ALM	Indicates unit is in alarm.
	LED, green/yellow	PSA	Indicates protection switch is active. LED is green if lighted on protection VTG, or LED is yellow if lighted on service VTGs.

* *The alarm LEDs (CR, MJ, and MN) on the COA are driven by alarm autonomous messages and entity states. If the primary state of the alarmed entity (equipment, for example) has been edited to OOS-MA and the state of an alarm condition changes for that entity, the changing of the alarm state is not reported until the entity is placed back in-service (primary state = IS). At that time, the autonomous message reporting of the alarm (or the clearing of the alarm) appears and the LED lights (or goes off). This action may lead to the false impression that the COA is not reporting alarms properly.*

TAP-001
Identify Alarms Using 1301 NMX

Purpose

Provides procedures for identifying alarms using 1301 NMX.

Prerequisites

This procedure assumes the 1301 NMX Explorer is installed on a 1603 SMX Network Element (NE) (referred to as the host NE) and is monitoring the network (PC Domain) for alarms.

Refer to DLP-300 to perform Network Discovery.

STEP	PROCEDURE
1	From the Explorer browser, discover network to get a list of all the NEs in the network [DLP-117].
2	Determine which NE has the highest level alarm and log on to this NE [DLP-117].
3	After logon has been established, retrieve alarms [DLP-100].
4	On the Monitor Alarms work view, note the alarm level (Critical, Major, or Minor) in the Severity column.

5 If there is more than one alarm, determine which alarm to clear first. Base the decision on the severity level and affect on service. (Clear service-affecting alarms with a high severity level first.) If necessary, the following list helps establish a priority order:

- Equipment alarms
- Traffic-carrying facility alarms (EC1, OC3, OC12, OC48, T1, T3)
- USRLAN arlams
- Sync alarms
- BLSR alarms
- STS1/STS3c/STS12c path alarms
- VT1.5 path alarms
- ATM Port alarms
- POS Port alarms
- AAL5 alarms
- ATM Processing Element alarms
- VPL path alarms
- VCL alarms
- All others

6 After deciding which alarm to clear first, note the alarm type in the Type column (e.g., EQPT, OC12, STS1, etc.).

7 Find the alarm type in Table A and go to the referenced procedure.

8 STOP. This procedure is complete.

Table A. Trouble Analysis Procedures

ALARM TYPES	PROCEDURE
AAL5	TAP-055
ATM Port	TAP-051
ATM Processor	TAP-052
BITS	TAP-012
BLSR	TAP-058
COM	TAP-016
EC1	TAP-022
ENV	TAP-020
EQPT	TAP-021
IPT	TAP-047
LAN	TAP-044
LLSDCC	TAP-032
LLSMLDCC	TAP-045
NETWORK	TAP-018
OC3, OC12, or OC48	TAP-029
PORT (CRAFT)	TAP-017
POSPORT	TAP-059
RMT	TAP-031
SML	TAP-033
STS1, STS3c, or STS12c	TAP-034
SYNCN (BITSSYNC)	TAP-013
SYNCN (NESYNC)	TAP-027
TADRMAP	TAP-046
T1 (DMI)	TAP-035
T1 (DS3/DS1 Transmux)	TAP-050
T3	TAP-043
USRLAN (LIF901)	TAP-056
USRLAN (LIFG01)	TAP-057
VCL	TAP-054
VPL	TAP-053
VT1	TAP-038
X.25	TAP-023

TAP-003
Clear Error Messages

Purpose

Provides procedure for clearing error messages.

STEP	PROCEDURE
1	See Table A for input errors codes; Table B for privilege errors codes; Table C for status error codes; and Table D for equipage error codes. ***NOTE:*** *An input error results from an incorrect TL1 command being sent to the NE; a wrong sequence in a request, such as a unit not being in the proper state, the configuration not being what is expected, or a failure.* ***NOTE:*** *Input errors (acronyms beginning with an I) are typically caused by syntax errors resulting from incorrect data in input data fields.*
2	For more information on resolving error codes, go to the corresponding TAPs: Input error codes – TAP-004 Privilege error codes – TAP-005 Status error codes – TAP-006 Equipage error codes – TAP-007
3	STOP. This procedure is complete.

Table A. Input Error Codes

CODE	DESCRIPTION
IBEX	Invalid, extra input block detected
IBMS	Input, block missing
IBNC	Input, block not consistent
ICNC	Input, command not consistent
ICNV	Input, command not valid
IDNV	Input, data not valid, or superfluous
IDRG	Input, data out of range
IIAC	Input, invalid access parameter
IICT	Input, invalid correlation tag
IIFM	Input, invalid data format
IIPG	Input, invalid parameter grouping
IISP	Input, invalid syntax or punctuation
IITA	Input, invalid target identifier
INUP	Input, non-null unimplemented parameter
IPEX	Invalid, extra input parameters detected
IPMS	Input, parameter missing
IPNC	Input, parameters not consistent
IPNV	Input, parameter not valid

Table B. Privilege Error Codes

CODE	DESCRIPTION
PICC	Privilege, invalid command code. The command entered is not executable because the session or user is not allowed to use the command that received the error.
PIMA	Privilege, invalid memory address. The address is not accessible by the session or user.
PIUC	Privilege, illegal user code. The user is trying to change own authorization levels with an ENT/ED command, or the stated user code is illegal.
PIUI	Privilege, illegal user identity. The user ID or password is not acceptable (illegal, wrong format, or password already used).
PLNA	Privilege, login not active. A command requiring logon was entered, but no logon session is active.

Table C. Status Error Codes

CODE	DESCRIPTION
SAAL	Status, already allowed
SABT	Status, command execution aborted
SAIN	Status, already inhibited
SAIS	Status, already in service
SAMS	Status, already in maintenance state
SAOP	Status, already operated using an OPR command; use an RLS command to release
SAPR	Status, already in primary role
SARB	Status, all system resources busy; try later
SARL	Status, already released using an RLS command
SAWS	Status, already in working state
SDAS	Status, diagnostics already started; wait for completion
SDFA	Status, duplex unit failed
SDLD	Status, duplex unit locked
SDNA	Status, duplex unit not available
SDNC	Status, data not consistent
SDNR	Status, data not ready
SNOS	Status, not currently out-of-service
SNPR	Status, not in protection state
SNRM	Status, system not in restoration mode
SNSR	Status, no switch request outstanding
SNVS	Status, not in valid state
SPFA	Status, protection unit failed
SPLD	Status, protection unit locked
SROF	Status, requested operation failed
SSRD	Status, switch request denied
SSTP	Status, stopped
SWFA	Status, working unit failed
SWLD	Status, working unit locked

Table D. Equipage Error Codes

CODE	DESCRIPTION
ENAC	Equipage, not equipped with alarm cutoff
ENDG	Equipage, not equipped with diagnostic capability
ENDS	Equipage, not equipped with duplex switching
ENEQ	Equipage, not equipped
ENMD	Equipage, not equipped with memory device
ENPM	Equipage, not equipped with performance monitoring
ENPS	Equipage, not equipped with protection switching
ENRI	Equipage, not equipped for retrieving specified information
ENRS	Equipage, not equipped for restoration
ENSI	Equipage, not equipped for setting specified information
ENSS	Equipage, not equipped with synchronization switching
EQWT	Equipage, wrong type

TAP-004
Clear Command Input Errors (Ixxx)

Purpose

Provides procedures to clear command input errors (Ixxx) that are generated when a command is entered incorrectly.

STEP	PROCEDURE
1	Identify the input error code from Table A.
2	Analyze the command input that caused the error; then go to the step indicated in Table A to clear the error.

Table A. Input Error Codes

CODE	REASON FOR ERROR	STEP
IBEX	Invalid, extra input block detected	3
IBMS	Input, block missing	3
IBNC	Input, block not consistent	3
ICNC	Input, command not consistent	3
ICNV	Input, command not valid	3
IDNV	Input, data not valid, or superfluous	6
IDRG	Input, data out of range	6
IIAC	Input, invalid access parameter	8
IICT	Input, invalid correlation tag	8
IIFM	Input, invalid data format	6
IIPG	Input, invalid parameter grouping	12
IISP	Input, invalid syntax or punctuation	3
IITA	Input, invalid target identifier	8
INUP	Input, non-null unimplemented parameter	12
IPEX	Invalid, extra input parameters detected	12
IPMS	Input, parameter missing	12
IPNC	Input, parameter not consistent	12
IPNV	Input, parameter not valid	12

Codes – IBEX, IBMS, IBNC, ICNC, ICNV, and IISP

NOTE: *These error codes indicate an extra colon (:) or absence of a colon is missing.*

3 Look for mixing of position and name-defined parameters within the same block (between colons/semicolons [;]).

4 Verify command per the 1603 SMX Commands and Messages manual.

5 STOP. This procedure is complete.

Codes – IDNV, IDRG, and IIFM

NOTE: *These error codes indicate data parameter values are not consistent with their positions or names.*

6 Verify command per the 1603 SMX Commands and Messages manual.

7 STOP. This procedure is complete.

Codes – IIAC, IICT, and IITA

NOTE: *These error codes indicate staging parameter tid, aid, or ctag are not correct.*

8 Verify site identification relative to the command to be executed.

9 Verify the aid allowable with the command or per the 1603 SMX Commands and Messages manual.

10 Check messages to ascertain the latest ctag.

11 STOP. This procedure is complete.

Codes – IIPG, INUP, IPEX, IPMS, IPNC, and IPNV

12 Is the error IIPG, INUP, IPEX, IPMS, IPNC, or IPNV?

If IIPG, go to step 13.
If INUP or IPMS, go to step 14.
If IPEX, go to step 15.
If IPNC or IPNV, go to step 16.

13 Check for improper use of the ampersand (&) per the 1603 SMX Commands and Messages manual.

14 Check for a required parameter that has not been entered per the 1603 SMX Commands and Messages manual, or enter command again.

15 Check for an extra parameter by comparing to the 1603 SMX Commands and Messages manual, or enter command again.

16 ***NOTE:*** *The parameter values or parameters are not consistent with each other.*

Check parameters per the 1603 SMX Commands and Messages manual, or enter command again.

17 STOP. This procedure is complete.

TAP-005
Clear Command Privileges Errors (Pxxx)

Purpose

Provides procedures for clearing command privileges errors (Pxxx).

STEP	PROCEDURE
1	***NOTE:*** *All privilege categories require a security level of 7. For additional information on Security/User Authorization, see 1603 SMX Commands and Messages manual.* Are you logged on to the alarmed NE? If yes, go to step 3. If no, go to step 2.
2	Log on to the NE [DLP-117].
3	***NOTE:*** *Command privileges errors are generated when an unauthorized entrance is made by a user or an interface.* Find the error code received in Table A, and go to the step indicated to resolve the error.

Table A. Privilege Error Codes

CODE	REASON FOR ERROR	STEP
PICC	Privilege, invalid command code. The command entered is not executable because the session or user is not allowed to use the command that received the error.	4
PIMA	Privilege, invalid memory address. The user is inhibited from accessing a memory location.	21
PIUC	Privilege, illegal user code. The user is trying to change own authorization levels with an ENT/ED command, or the stated user code is illegal.	25
PIUI	Privilege, illegal user identity. A user without the proper privileges tried to execute a command.	33
PLNA	Privilege, logon not active. A command requiring logon was entered, but no logon session is active.	23

Code – PICC

4 Retrieve security levels associated with command that received the error [DLP-520].

NOTE: *The security categories are PCMAINT (Maintenance Privilege Code with levels 0-7); PCPROV (Provisioning Privilege Code, 0-7); PCSECU (Security Privilege Code, 0-7); and PCTEST (Test Privilege Code, 0-7).*

5 Record the four command privilege codes.

6 Retrieve user's security privilege codes [DLP-520].

7 Record the four user privilege codes; then close work view.

8 Align the categories of step 7 above step 5. Refer to Table B for example.

Table B. Comparison Between User and Command Privilege Codes

STEP	M	P	S	T
Step 7 (user)	5	5	4	5
Step 5 (command)	0	0	7	0

9 Is there a category in which there is comparison between non-zeroes?

If yes, go to step 11.
If no, execution is denied. See the system administrator.

10 STOP. This procedure is complete.

11 Are any command categories higher than corresponding user categories?

If yes, see the system administrator.
If no, go to step 12.

12 Retrieve security privilege codes for port used to log on [DLP-520].

13 Record the Maintenance, Provisioning, Security, and Test Privilege Codes for the port through which you are logged on to the NE.

14 Align the categories of step 13 above step 5. Refer to Table C for example.

Table C. Comparison Between Port Access and Command Privilege Codes

STEP	M	P	S	T
Step 13 (port access)	4	4	4	4
Step 5 (command)	0	0	7	0

15 Is there a category in which there is a comparison between non-zeroes?

If yes, go to step 16.
If no, go to step 17.

16 Are any command categories higher than corresponding port access categories?

If yes, go to step 17.
If no, go to step 19.

17 Execution is denied. See the system administrator or go to another Access Type port.

18 STOP. This procedure is complete.

19 ***NOTE:*** *If the user and port access are higher in all categories that are compared, then execution should not be denied.*

If other alarms exist, go to TAP-001.

20 STOP. This procedure is complete.

Code – PIMA

21 If the user requires access, contact the system administrator.

22 STOP. This procedure is complete.

Code – PLNA

23 ***NOTE:*** *A PLNA error indicates that a command requiring a log on session was entered, but no logon session is active.*

Log on to the NE [DLP-117].

24 STOP. This procedure is complete.

Code – PIUC

25 Retrieve user's security privilege codes [DLP-520].

26 Record the levels of the Maintenance, Provisioning, Security, and Test privilege codes; then close work view.

27 Are the codes correct (0-7)?

If yes, go to step 30.
If no, go to step 28.

28 Have the system administrator change the user privilege codes [DLP-520].

29 STOP. This procedure is complete.

30 ***NOTE:*** *If you are authorized to enter an ED/ENT-SECU command, you may be demoting your code levels.*

Compare command input data from the command that was alarmed to that retrieved (step 26).

31 Have system administrator enter correct data.

32 STOP. This procedure is complete.

Code – PIUI

This type of privilege error indicates that a user without the proper privileges tried to execute a command. Some of the possible causes for this type of error are as follows:

- The User ID, with the password used, may not be correct.
- The password may have been assigned to someone else.
- The password entered has illegal characters (6 to 10 alphanumeric characters with minimum of one numeric and one non-TL1 symbolic character; e.g., ~ @ # $ % ^ + - _ =).
- The User ID Aging Interval or Password Aging Interval has expired.

33 Have the system administrator retrieve the user privilege codes and make the necessary changes [DLP-520].

34 STOP. This procedure is complete.

TAP-006
Clear Command Status Errors (Sxxx)

Purpose

Provides procedures for clearing command status errors (Sxxx).

STEP	PROCEDURE

1 ***NOTE:*** *Command status errors are generated when a command is not executed due to the status of the system.*

Are you logged on to the alarmed NE?

If yes, go to step 3.
If no, go to step 2.

2 Log on to the NE and open 1603 SMX Application browser [DLP-117].

3 Find the status error code in Table A and go to the step indicated to resolve the error.

Table A. Status Error Codes

CODE	REASON FOR ERROR	STEP
SAAL	Status, already allowed	4
SABT	Status, command execution aborted	7
SAIN	Status, already inhibited	4
SAIS	Status, already in-service	4
SAMS	Status, already in maintenance state	4
SAOP	Status, already operated using an OPR command; use an RLS command to release	–
SAPR	Status, already in primary role	4
SARB	Status, all system resources busy; try later	–
SARL	Status, already released via an RLS command	–
SAWS	Status, already in working state	4
SDAS	Status, diagnostics already started; wait for completion	–
SDFA	Status, duplex unit failed	7
SDLD	Status, duplex unit locked	12

Table A. Status Error Codes (cont)

CODE	REASON FOR ERROR	STEP
SDNA	Status, duplex unit not available	4
SDNC	Status, data not consistent	15
SDNR	Status, data not ready	18
SNOS	Status, not currently out-of-service	4
SNPR	Status, not in protection state	4
SNRM	Status, system not in restoration mode. An INH-AUTORST command probably was executed, inhibiting synchronization restoration.	21
SNSR	Status, no switch request outstanding	23
SNVS	Status, not in valid state	4
SPFA	Status, protection unit failed	7
SPLD	Status, protection unit locked	12
SROF	Status, requested operation failed	7
SSRD	Status, switch request denied	4
SSTP	Status, stopped	7
SWFA	Status, working unit failed	7
SWLD	Status, working unit locked	12

Codes – SAAL, SAIN, SAIS, SAMS, SAPR, SAWS, SDNA, SNOS, SNPR, SNVS, and SSRD

4 Do you want to verify the status or state of the entity?

If yes, go to step 5.
If no, STOP. This procedure is complete.

5 Determine the service state of the entity reporting the error [DLP-501].

6 From the status of states, do you want to pursue or correct the status?

If yes, go to IXL-001.
If no, STOP. This procedure is complete.

Codes – SABT, SDFA, SPFA, SROF, SSTP, and SWFA

7 Retrieve alarms [DLP-100].

8 Are any alarm conditions indicated?

If yes, go to TAP-001.
If no, go to step 9.

9 ***NOTE:*** *The command relates to one or more units.*

NOTE: *Always give precedence to PWR, CLK, and NEP alarms; then DMI, HIF, and CCM equipment alarms; then facility, path, and miscellaneous alarms.*

Determine which unit(s) are involved and interrogate those units.

10 Select the most likely unit and replace it per DLP-101.

11 STOP. This procedure is complete.

Codes – SDLD, SPLD, and SWLD

12 Do you want to unlock the unit/facility?

If yes, go to step 13.
If no, STOP. This procedure is complete.

13 Select the entity you want to unlock from the following list:

- To allow switching to redundant DMI, CCM, CLK, or LIF, refer to DLP-506.
- To allow switching to redundant LDR101/201/301, refer to DLP-506.
- To allow switching of LDR501 to protection, refer to DLP-535.
- To allow switching of VTG to protection, refer to DLP-535.
- To allow protection switching on facilities, refer to DLP-545.
- To allow protection switching on paths, refer to DLP-507.

14 STOP. This procedure is complete.

Code – SDNC

15 Check parameters and values of parameters.

16 ***NOTE:*** *For assistance, see the 1603 SMX Commands and Messages manual.*

Reenter the command.

17 STOP. This procedure is complete.

Code – SDNR

18 ***NOTE:*** *The entity is not ready to accept commands. Reenter command later.*

Determine service state of the entity reporting the error [DLP-501].

19 Retrieve all active alarms to determine if any alarm has inhibited the retrieval [DLP-100].

20 STOP. This procedure is complete.

Code – SNRM

21 To clear the error code, allow automatic synchronization restoration [DLP-558].

22 STOP. This procedure is complete.

Code – SNSR

23 ***NOTE:*** *This error code indicates an attempt was made to release a switch that has no switch request outstanding. No action is necessary.*

STOP. This procedure is complete.

TAP-007
Clear Command Equipage Errors (Exxx)

Purpose

Provides procedures for clearing command equipage errors (Exxx).

STEP	PROCEDURE

1 ***NOTE:*** *Command equipage errors are generated when a command cannot be executed because the system is not equipped to satisfy the functional requirement.*

Are you logged on to the alarmed NE?

If yes, go to step 3.
If no, go to step 2.

2 Log on to the NE [DLP-117].

3 Identify the equipage error code from Table A.

Table A. Equipage Error Codes

CODE	REASON FOR ERROR
ENAC	Not equipped with alarm cutoff
ENDG	Not equipped with diagnostic capability
ENDS	Equipage, not equipped with duplex switching
ENEQ	Equipage, not equipped
ENMD	Equipage, not equipped with memory device
ENPM	Equipage, not equipped with performance monitoring
ENPS	Equipage, not equipped with protection switching
ENRI	Equipage, not equipped for retrieving specified information
ENRS	Equipage, not equipped for restoration
ENSI	Equipage, not equipped for setting specified information
ENSS	Equipage, not equipped with synchronization switching
EQWT	Equipage, wrong type

4 Verify the secondary state equipage for the unit in question:

a. In the scope pane, expand Equipment and select unit being checked (LIF, HIF, NEP, etc.).

b. In the result pane, note status of secondary state.

5 Retrieve hardware inventory [DLP-537].

6 On the Hardware Inventory work view, check functionality of unit; then reference applicable Unit Data Sheet in the 1603 SMX Product Information manual.

7 By description of equipage code, determine what action to take.

8 STOP. This procedure is complete.

TAP-010
Clear Alarm Using Visual Indicators

Purpose

To provide a procedure for clearing an alarm if a terminal or a PC is not available and you cannot communicate with the NE using the craft port.

General

It is recommended that alarm messages be analyzed to determine problems. Use this procedure only if a terminal or PC is not available or communication with craft port has failed. Also, craft port access may be required to download software to the replacement unit.

When replacing plug-in units, a few minutes may be required for the system to stabilize and alarms to clear. If alarms do not clear, replace the original unit before replacing another unit.

STEP	PROCEDURE
1	**CAUTION: Possibility of service interruption. Replacing plug-in units without first analyzing alarm messages may cause unnecessary service interruptions.**
2	Review handling of static sensitive plug-in units [DLP-518].
3	Is a PC with means for logging on to the Network Element (NE) available? If yes, go to step 4. If no, go to step 5.
4	Can you communicate with NE? If yes, go to TAP-001. If no, go to TAP-039.
5	If necessary, review shelf layout (Figure 1) and system block diagram (Figure 2).
6	If not already done, silence office alarms by pressing Alarm Cut-off (ACO) button on COAxxx plug-in (COA) unit (Figure 3).
7	Determine which plug-in LEDs are lighted. Refer to Table A for a description of the LEDs and Table B for a list of the conditions that light the ABN LED on an NEP.

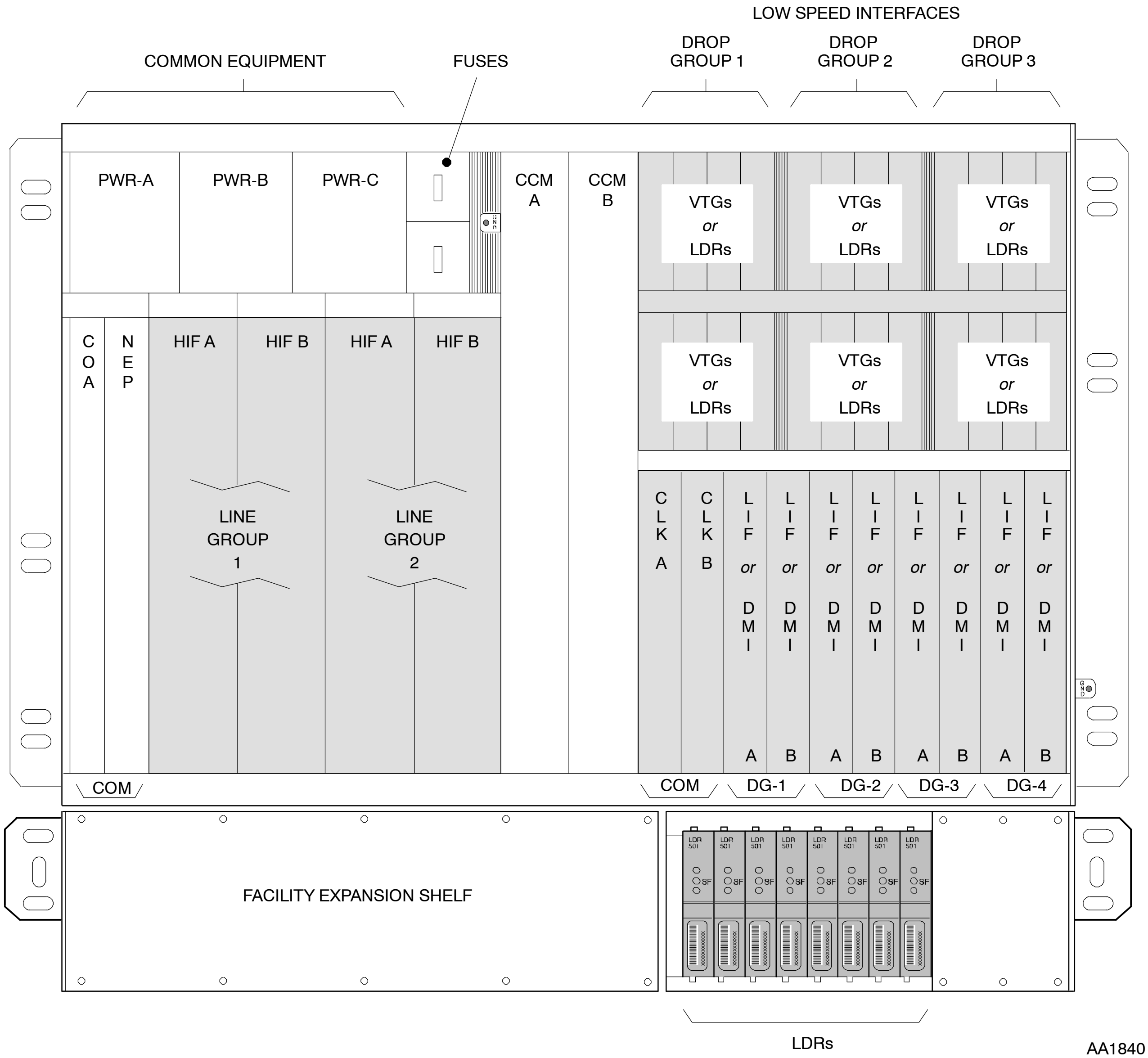


Figure 1. 1603 SMX Shelf Layout

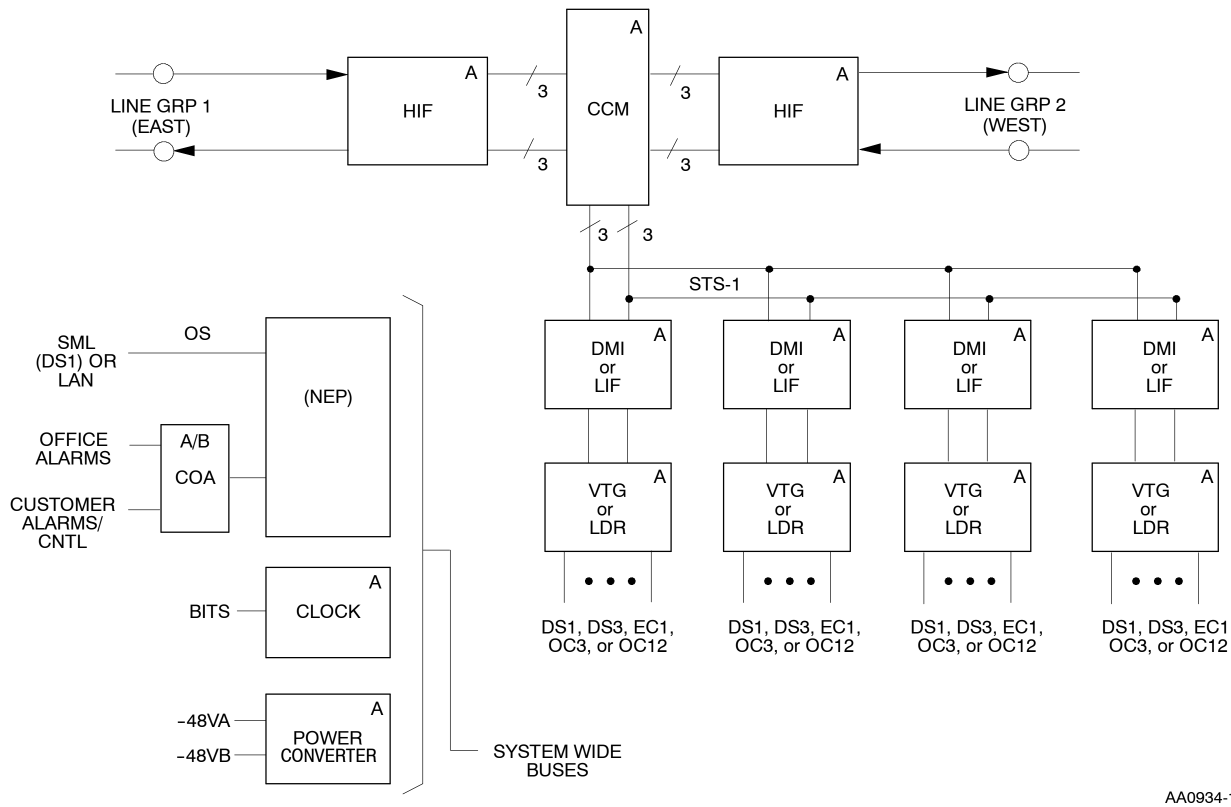


Figure 2. 1603 SMX Functional Block Diagram – A-Side Equipment

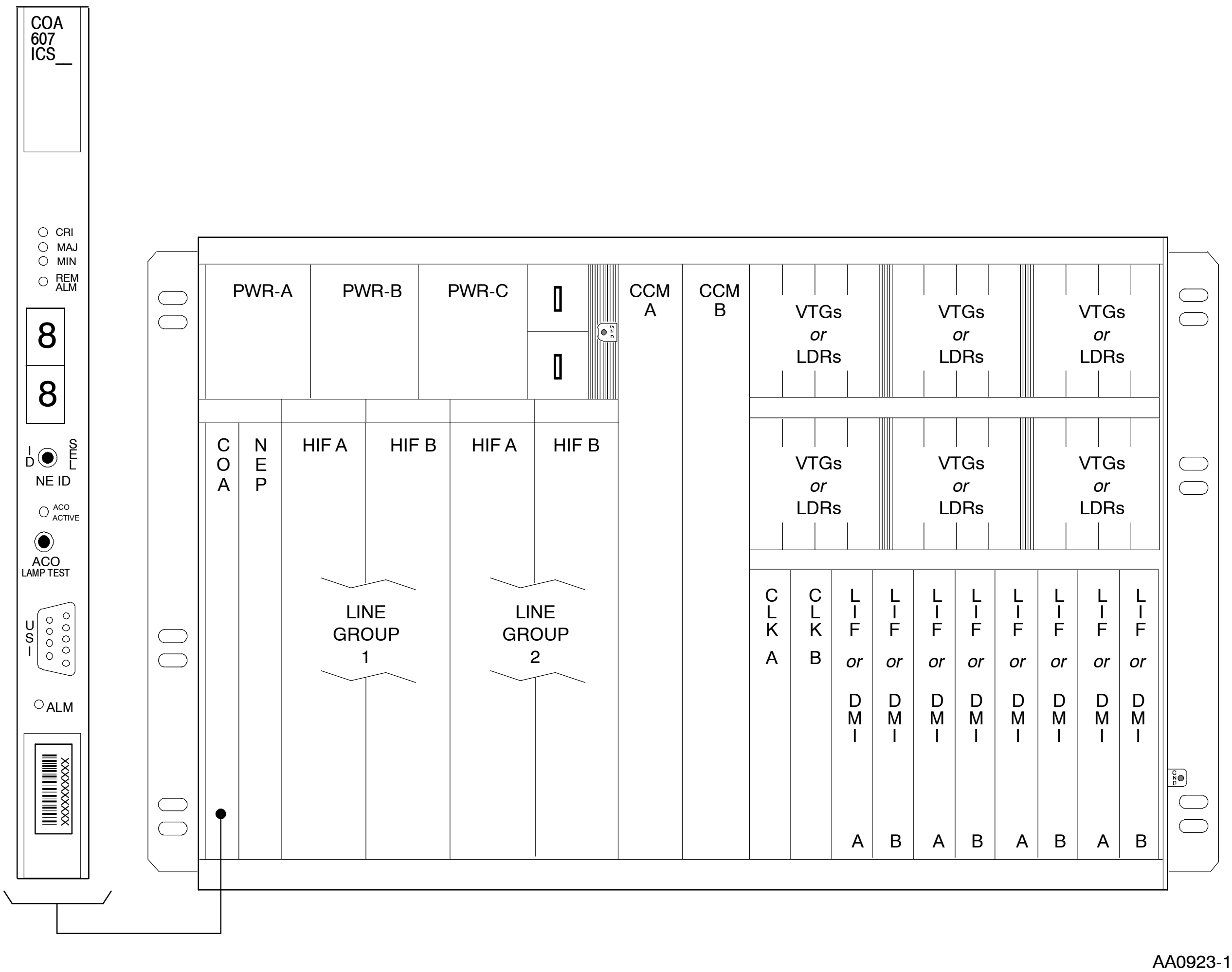


Figure 3. COAxxx Plug-in Unit

Table A. 1603 SMX Plug-in Alarm Indicators

UNIT/LED	INDICATION WHEN LED IS LIGHTED	PROBABLE CAUSE/CORRECTIVE ACTION
COAxxx Craft, Orderwire and Alarm Unit		
CRI	Critical alarm level	Provides system alarm severity level
MJ	Major alarm level	Provides system alarm severity level
MN	Minor alarm level	Provides system alarm severity level
REM ALM	Remote (Far-End) alarm is present	Push ID SEL button to cycle through list of FEADISPNUMs reporting alarms to this NE
NE ID Seven-Seg ment LED Display	When ID SEL button is pushed, remote NE FEADISPNUMs are displayed along with active alarms indicated by CRI, MJ and MN LEDs	Determine what NE name (from office records) is associated with FEADISPNUM. Go to, or log on to, alarmed NE to resolve alarm(s)
ACO ACTIVE	Alarm cutoff has been activated	Silences office alarms, no action required
ALM	Unit failure	**CAUTION: Possibility of service interruption. See TAD-001 for database information before replacing unit.** Replace unit per DLP-101
NEPxxx Network Element Processor Unit		
ACT	Unit is active	Not an alarm, status indicator only
ABN	Abnormal condition exists in NE, or unit is running bootcode if flashing	An equipment or facility has been placed in an abnormal state or NEP is running bootcode. Refer to Table B
ALM	Unit failure	**CAUTION: Possibility of service interruption. See TAD-001 for database information before replacing unit.** Replace unit per DLP-101
HIFxxx High Speed Interface Unit (OC3, OC12 and OC48)		
ACT	Unit is active	Not an alarm, status indicator only
SF	Incoming signal failure	Check facility, far-end NE, near-end and far-end facility provisioning
ALM	Unit failure	Replace unit per DLP-101
CLK20x Clock Unit		
ALM	Unit failure	Replace unit per DLP-101
DMIxxx Drop Module Interface Unit		
ACT	Unit is active	Not an alarm, status indicator only
ALM	Unit failure	Replace unit per DLP-101

Table A. 1603 SMX Plug-in Alarm Indicators (cont)

UNIT/LED	INDICATION WHEN LED IS LIGHTED	PROBABLE CAUSE/CORRECTIVE ACTION
VTGxxx Virtual Tributary Group (Asynchronous DS1) Unit		
SF	Signal failure on any or all of four DS1s served by unit	Check DS1 facility, far-end multiplexer equipment
ALM	Unit failure	**CAUTION: Possibility of service interruption. VTG with ALM lighted may be providing access to protection VTG for another unit and may interrupt service on that unit.** Replace unit per DLP-101
PSA	Protection switch active (not available on VTG101)	Indication only. Look for other alarms
LIF20x/30x/50x/601/701/D01 Low Speed Interface Unit		
ACT	Unit is active	Not an alarm, status indicator only
ALM	Unit failure	Replace unit per DLP-101
LIF40x/A0x		
ACT	Unit is active	Not an alarm, status indicator only
SF	Incoming signal failure	Check facility provisioning – NE and FE
ALM	Unit failure	Replace unit per DLP-101
LIF901		
ALM	Unit failure	Replace unit per DLP-101
SF -1, -2, -3, -4	Ethernet port failure	Check facility provisioning – NE and FE
LIFF01		
ACT	Unit is active	Not an alarm, status indicator only
ALM	Unit failure	Replace unit per DLP-101
SF -1, -2, -3, -4	OC3 facility signal failure	Check facility provisioning – NE and FE
LIFG01		
ACT	Unit is active	Not an alarm, status indicator only
SF	Incoming signal failure	Check facility provisioning
ALM	Unit failure	Replace unit per DLP-101

Table A. 1603 SMX Plug-in Alarm Indicators (cont)

UNIT/LED	INDICATION WHEN LED IS LIGHTED	PROBABLE CAUSE/CORRECTIVE ACTION
LDR101/201/301 Line Driver Unit		
ACT	Unit is active	Not an alarm, status indicator only
SF	Incoming signal failure	Check facility provisioning – NE and FE
ALM	Unit failure	Replace unit per DLP-101
LDR501 Line Driver Unit		
PSA	Protection switch active	Indication only. Look for other alarms
SF	Incoming signal failure on either facility	Check facility provisioning – NE and FE
ALM	Unit failure	Replace unit per DLP-101
PWRA01 Power Converter Unit		
ON	-48 Vdc power is provided to unit	Not an alarm; normal indication. If off, -48 Vdc input is not present
ALM	Unit failure	Replace unit per DLP-101
CCMx01 Cross-Connect Unit		
ACT	Unit is active	Not an alarm, status indicator only
ALM	Unit failure	Replace unit per DLP-101

Table B. Conditions that Light the ABN LED on NEP

CONDITION	REASON FOR ABNORMAL CONDITION
BOOT	Processor unit is running bootcode
CONFIG	Configuration error (usually encountered during upgrade)
FRCD/MAN	Forced or manual switch request on an OCn line or an STS or VT1 path
FRCD-RING	Forced BLSR switch ring request
MAN-RING	Manual BLSR switch ring request
FWMJVER	Firmware major version error (LIF901)
INHAUTOMODESW	Auto switching back to primary timing reference when returning to normal is inhibited
INHSWDX	Switch to duplex equipment is inhibited
INHSWPR	Switch to protection equipment inhibited
INHSWWKG	Switch to working equipment inhibited
LOCKOUT	STS or VT1 path switch is locked out
LOCKOUT-LOWR	A BLSR ring lockout switch request is in effect for the local NE
LOCKOUT-LPS	A BLSR ring lockout switch request is in effect for the entire ring
LOCKOUTOFPR	OC3, OC12, or OC48 facility APS locked out of protection
MTCE	Equipment or facility is in maintenance state (OOS-MT)
OPRACT	Sync. reference switch is in effect because of operator action
PROGVER	Slave-processor unit has different program version than NEP

8 Are any LEDs lighted besides the CRI, MJ, and MN LEDs on the COA?

If yes, go to step 10.
If no, go to step 9.

9 ***NOTE:*** *Craft terminal or PC is required for further analysis.*

Go to TAP-001.

10 Is the ALM (red) LED lighted on any of the units?

If yes, go to step 11.
If no, go to step 15.

11 **CAUTION: Possibility of service interruption. Refer to Table A for any warnings or cautions pertaining to replacement plug-in unit before proceeding.**

12 ***NOTE:*** *If NEP, HIF, LIF, or DMI is replaced, unit may require software to be downloaded, which requires a Personal Computer. Refer to DLP-566.*

Replace the unit with the lighted ALM (red) LED.

13 After several minutes, did the unit ALM (red) LED go off?

If yes, STOP. This procedure is complete.
If no, go to step 14.

14 ***NOTE:*** *Craft terminal or PC is required for further analysis.*

Go to TAP-001.

15 Select the LED that is lighted:

If NEP ABN LED, go to step 16.
If HIF or LIF (OC3/OC12/OC48) SF LED, go to step 17.
If VTG or LDR SF LED, go to step 18.

16 ***NOTE:*** *Abnormal state exists in the NE as listed in Table B. A craft terminal is required for further analysis.*

Go to TAP-001.

17 ***NOTE:*** *Indicates a signal fail condition has been detected on the OC3, OC12, or OC48 facility. A craft terminal is required for further analysis.*

Go to TAP-001.

18 ***NOTE:*** *Indicates a signal fail condition has been detected on the T1 (VTG) or EC1/T3 (LDR) facility. A craft terminal is required for further analysis.*

Go to TAP-001.

19 STOP. This procedure is complete.

TAP-012
Clear BITS Alarm (Input)

Purpose

Provides a procedure for clearing a BITS alarm (input).

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific Network Elements (NEs).

STEP	PROCEDURE
1	Retrieve alarms [DLP-100].
2	Locate the alarm or condition in Table A; then go to the step indicated to clear it.

Table A. Bits Alarms/Conditions/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
AIS	Alarm Indication Signal. A code (all ones) has been sent downstream to indicate that an upstream failure has been detected. This code has been detected on an incoming SYNCPRI/SYNCSEC BITS DS1 facility.	3
AISYEL	Alarm Indication Signal — Yellow. This is a status condition for alerting upstream equipment that an AIS has been received in the downstream equipment.	4
BER-HT	A Bit Error Ratio-High Threshold was exceeded	5
LOF	Loss of Frame. Excessive amount of out-of-frame occurrences have taken place on the incoming DS1 reference signal. An LOF condition occurs when a Severely Errored Frame (SEF) defect is detected on the incoming signal.	17
LOS	Loss of Signal	5
MTCE	BITS facility has been placed in maintenance state.	30
SYNCLEVINFAIL	Synchronization level input failure. NE received an invalid synchronization message value or constantly changing values from the BITS source. Valid values are 2, 4, 6, 8, 17, 20, 24, and 32 for first generation of synchronization message level, and valid values are 2, 4, 6, 8, 17, 20, 24, 32, 60, and 62 for second generation of synchronization message level.	32

Table A. Bits Alarms/Conditions/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
YEL	Yellow. The NE has received a notification from the BITS that there is a downstream failure (probably between the BITS and this NE).	50
Condition	**Description**	**Step**
SYNCLEVIN-( )	Synchronization input level	No action
SYNCLEVOUT-( )	Synchronization output level	No action
Event	**Description**	**Step**
SYNCLEVINCHG	Synchronization level input change	No action

Alarm/Condition – AIS

3 ***NOTE:*** *The problem is not in this NE. The AIS signal, which is received through the Sync unit BITS DS1 input, is being generated by equipment external to this NE, (i.e., Building Integrated Timing Supply) and external to this network.*

STOP. This procedure is complete.

Alarm/Condition – AISYEL

4 ***NOTE:*** *AISYEL is not typically transmitted by BITS sources. Suspect obscure wiring or BITS or timing source problems.*

STOP. This procedure is complete.

Alarm/Condition – BER-HT and LOS

5 Retrieve alarms [DLP-100].

6 Are there any CLK alarms?

If yes, go to TAP-014.
If no, go to step 7.

7 Check equalization distance at other NE [DLP-531].

8 Is equalization distance correct?

If yes, go to step 11.
If no, go to step 9.

9 Change equalization distance [DLP-531]; then retrieve alarms [DLP-100].

10 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 11.

11 Verify there is a good wire-wrap connection on the IN SYNCPRI or SYNCSEC per the response. See Figure 1.

12 Is the connection good?

If yes, go to step 15.
If no, go to step 13.

13 Redo the connection.

14 STOP. This procedure is complete.

15 ***NOTE:*** *The problem is from the sync source specified by the alarm.*

Troubleshoot problem at the source.

16 STOP. This procedure is complete.

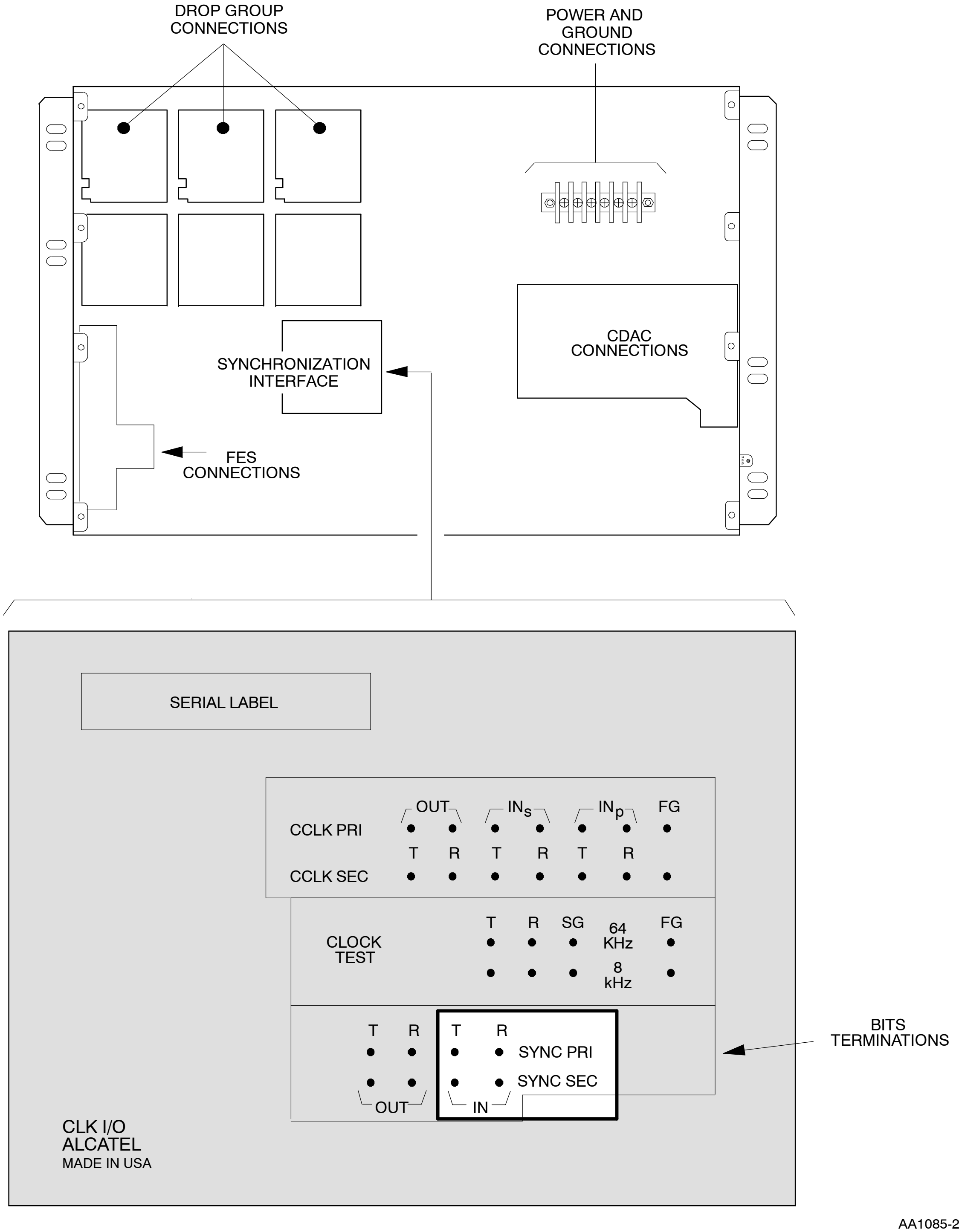


Figure 1. Rear View, Section 1 Cabling

Alarm/Condition – LOF

17 Retrieve alarms [DLP-100] and note whether alarm is being generated by SYNCPRI or SYNCSEC.

18 Are there any CLK alarms?

If yes, go to TAP-021.
If no, go to step 19.

19 Check the wire-wrap connection on the SYNCPRI or SYNCSEC pins on the IN side. See Figure 1.

20 Is the connection good?

If yes, go to step 23.
If no, go to step 21.

21 Redo the connection.

22 STOP. This procedure is complete.

23 Check NE BITS provisioning against BITS equipment provisioning to ensure that Frame Format and Line Code are in agreement on the two pieces of equipment [DLP-539].

24 Are Frame Format and Line Code parameters correct?

If yes, go to step 28.
If no, go to step 25.

25 Change Frame Format and Line Code parameters [DLP-539].

26 Retrieve alarms [DLP-100].

27 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 28.

28 ***NOTE:*** *The problem is from the sync source specified by the alarm.*

Check equalization at BITS equipment; correct if necessary. Troubleshoot problem at the source.

29 STOP. This procedure is complete.

Alarm/Condition – MTCE

30 To clear alarm, place the BITS facility back in-service [DLP-501].

31 STOP. This procedure is complete.

Alarm/Condition – SYNCLEVINFAIL

32 Retrieve current BITS synchronization conditions [DLP-100].

33 Note the number following **SYNCLEVIN**.

NOTE: *The number following SYNCLEVIN is the synchronization status message (expressed as a decimal number). This message is contained in the ESF datalink message.*

34 Is synchronization status message a valid value (2, 4, 6, 8, 17, 20, 24, 32, 60, or 62)?

If yes, go to step 35.
If no, go to step 43.

35 In the first column of Table B, find the value obtained in step 33.

NOTE: *The other two columns define the quality level and the sync traceability that correspond to that synchronization message value.*

Table B. Interpretation of SYNCLEVIN Message Values

SYNCHRONIZATION STATUS MESSAGE	QUALITY LEVEL		SYNCHRONIZATION TRACEABILITY
	1ST GENERATION (V1)	2ND GENERATION (V2)	
2	1	1	Stratum 1 Traceable
4	2	2	Traceability Unknown
6	3	3	Stratum 2 Traceable
8	4	6	Stratum 3 Traceable
17	5	7	Minimum Clock Traceable
20	6	8	Stratum 4 Traceable
24	7	9	Don’t use for synchronization
32	User assignable	User assignable	Reserved for network sync
60	N/A	4	Transit Node Clock Traceable
62	N/A	5	Stratum 3E Traceable

36 Is the quality level 1, 2, 3, or 4?

If no, go to step 38.
If yes, go to step 40.

37 Network synchronization provisioning is probably not correct.

38 ***NOTE:*** *Network synchronization provisioning is probably not correct.*

Contact Customer Service.

39 STOP. This procedure is complete.

40 Retrieve synchronization conditions [DLP-100].

41 Is the synchronization value the same as it was before (step 33)?

If yes, contact Customer Service.
If no, the synchronization value is changing. Go to step 43.

42 STOP. This procedure is complete.

43 Retrieve alarms [DLP-100].

44 Are there any CLK alarms?

If yes, go to TAP-021.
If no, go to step 45.

45 Check the wire-wrap connection on the SYNCPRI or SYNCSEC pins on the IN side. See Figure 1.

46 Is the connection good?

If yes, go to step 48.
If no, correct the connection.

47 STOP. This procedure is complete.

48 ***NOTE:*** *The problem is from the sync source specified by the alarm.*

Troubleshoot problem at the source.

49 STOP. This procedure is complete.

Alarm/Condition – YEL

50 ***NOTE:*** *Far-end equipment generates a yellow signal for a variety of conditions. Since the far-end equipment could be another vendor's, this procedure cannot identify specific alarms at the other end.*

Retrieve alarms [DLP-100].

51 Are there any CLK alarms?

If yes, go to TAP-021 and clear CLK alarm(s).
If no, go to step 52.

52 Check the wire-wrap connection on the SYNCPRI or SYNCSEC pins on the IN side. See Figure 1.

53 Is the connection good?

If yes, go to step 55.
If no, correct the connection.

54 STOP. This procedure is complete.

55 Suspect equipment or facility problems. Go to TAP-001.

56 STOP. This procedure is complete.

TAP-013
Clear Output Sync Alarm (BITS Output)

Purpose

Provides procedures for clearing an output sync alarm (BITS output).

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific Network Elements (NEs).

STEP	PROCEDURE
1	Have alarms been retrieved? If yes, go to step 3. If no, go to step 2.
2	Retrieve alarms [DLP-100].
3	Locate the alarm or condition in Table A; then go to the step indicated to clear it.

Table A. Output SYNC (BITS) Alarms/Conditions/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
PRI-DG1A-n	A primary reference failure has occurred on Drop Group 1, Side A, Facility 1…4.	4
PRI-DG1B-n	Primary reference failure – Drop Group 1, Side B, Facility 1…4	4
PRI-DG2A-n	Primary reference failure – Drop Group 2, Side A, Facility 1…4	4
PRI-DG2B-n	Primary reference failure – Drop Group 2, Side B, Facility 1…4	4
PRI-DG3A-n	Primary reference failure – Drop Group 3, Side A, Facility 1…4	4
PRI-DG3B-n	Primary reference failure – Drop Group 3, Side B, Facility 1…4	4
PRI-DG4A-n	Primary reference failure – Drop Group 4, Side A, Facility 1…4	4
PRI-DG4B-n	Primary reference failure – Drop Group 4, Side B, Facility 1…4	4
PRI-LG1A	A primary reference failure has occurred on Line Group 1, Side A	10

Table A. Output SYNC (BITS) Alarms/Conditions/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
PRI-LG1B	Primary reference failure – Line Group 1, Side B	10
PRI-LG2A	Primary reference failure – Line Group 2, Side A	10
PRI-LG2B	Primary reference failure – Line Group 2, Side B	10
INHAUTOMODESW	Inhibit Auto Mode Switching. Automatic restoration of BITSSYNC is inhibited	15
LOCKOUTOFSYNC	Lockout of Synchronization. Synchronization reference switching is locked.	17
OPRACT	Operate Active. A manual switch to a synchronization reference is in effect.	22
SYNCSWFAIL	Synchronization reference switch failure	26
Condition	**Description**	**Action**
OPRSYNC-PRI	Operate synchronization on primary reference	No action
OPRSYNC-SEC	Operate synchronization on secondary reference	No action
Event	**Description**	**Action**
MANSWTOPRI	Manual switch to primary reference	No action
MANSWTOSEC	Manual switch to secondary reference	No action
SWTOPRI	Automatic switch to primary reference	No action
SWTOSEC	Automatic switch to secondary reference	No action

Alarm/Condition – PRI-DGxx

4 Retrieve alarms [DLP-100].

5 Are there any CLK, LIF, or NEP alarms?

If yes, go to TAP-021 and clear alarms.
If no, go to step 6.

6 Are there any OC3 or OC12 facility alarms?

If yes, go to TAP-029 and clear OC facility alarm(s).
If no, go to step 7.

7 Are there any EC1 facility alarms?

If yes, go to TAP-022 and clear EC1 facility alarm(s).
If no, go to step 8.

8 Contact Customer Service.

9 STOP. This procedure is complete.

Alarm/Condition – PRI-LGxx

10 Retrieve alarms [DLP-100].

11 Are there any CLK, HIF, or NEP alarms?

If yes, go to TAP-021 and clear alarms.
If no, go to step 12.

12 Are there any line group OC3, OC12, or OC48 alarms?

If yes, go to TAP-029 and clear OC facility alarm(s).
If no, go to step 13.

13 Contact Customer Service.

14 STOP. This procedure is complete.

Alarm/Condition – INHAUTOMODESW

15 To clear alarm, allow automatic restoration of BITS sync [DLP-558].

16 STOP. This procedure is complete.

Alarm/Condition – LOCKOUTOFSYNC

17 ***NOTE:*** *After 4 hours of a continuous LOCKOUTOFSYNC state, the NE clears automatically.*

Do you want to switch to a preferred source?

If yes, go to step 18.
If no, STOP. This procedure is complete.

18 Switch to an alternate BITS timing reference and release [DLP-503].

19 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 20.

20 Suspect synchronization source problems. Select path of sync source(s) used.

If LGx, go to step 10.
If DGx, go to step 4.

21 STOP. This procedure is complete.

Alarm/Condition – OPRACT

22 **CAUTION: Possibility of service interruption. While the OPRACT alarm is active, normal synchronization switching is inhibited. Do not leave OPRACT alarm active during normal operation.**

23 Is there a valid reason to keep BITS sync manually switched?

If yes, STOP. This procedure is complete.
If no, go to step 24.

24 Release the BITS timing reference [DLP-503].

25 STOP. This procedure is complete.

Alarm/Condition – SYNCSWFAIL

26 Retrieve alarms [DLP-100].

27 Are there any equipment alarms?

If yes, go to step 28.
If no, go to step 31.

28 ***NOTE:*** *All unit alarms are indicated on the COA unit by severity level (i.e., CR [Critical], MJ [Major], or MN [Minor]). If there is a COA CONTCOM and an NEP alarm, resolve the COA alarm first.*

Identify the alarmed unit with the highest severity.

29 Go to TAP-021 to clear equipment alarms. Clear highest severity alarms first (i.e., CR, MJ, etc.).

30 STOP. This procedure is complete.

31 Are there any facility alarms?

If yes, go to TAP-001.
If no, go to step 32.

32 Switch the BITS timing reference and release [DLP-503].

33 Wait approximately one minute; then retrieve alarms [DLP-100].

34 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 35.

35 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid interrupting service.**

36 Replace active CLK per DLP-101; then retrieve alarms [DLP-100].

37 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 38.

38 Contact Customer Service.

39 STOP. This procedure is complete.

TAP-016
Clear Common (COM) NE Alarm

Purpose

Provides procedures for clearing a common (COM) NE alarm.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Have the alarms been retrieved? If yes, go to step 3. If no, go to step 2.
2	Retrieve common alarms [DLP-100].
3	Locate alarm or condition in Table A; then go to the referenced step to clear it.

Table A. Common NE Alarms/Conditions/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
ALMSYNC	Alarms are out-of-sync with COA LEDs	4
BAFFLEALM1	Baffle Alarm 1. A cable on the baffle trap door has failed.	7
BAFFLEALM2	Baffle Alarm 2. A cable on the baffle trap door has failed.	7
CONFIG	Configuration error. During the upgrade process, a mismatch was detected between Side A and Side B equipment that was provisioned in DUPLEX mode.	9
EQPTMA	One or more assigned plug-in units are OOS-MA (Memory Admin).	17
FA	Fuse alarm. A blown fuse on the 1603 SMX shelf fuse card has been detected.	23
FACMA	Assigned facility is OOS-MA-AS. All facilities should be placed in-service or entity alarms will not be reported.	20

Table A. Common NE Alarms/Conditions/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
FANALM	A rack/bay fan assembly alarm has been detected	33
INVERR	Inventory error. Contents of backplane Fuse Alarm Unit (FAU) inventory data are inconsistent or absent due to EEPROM communication problem.	35
LOGBUFR90-SECURITY	Security log buffer is 90% full	39
LOGBUFROVFL-SECURITY	Security log buffer is overflowing	39
LOGBUFR90-SYSTEM	System message log buffer is 90% full	42
LOGBUFROVFL-SYSTEM	System message log buffer is overflowing	42
MEA	The version of software the NEP is running doesn't support the 1603 SMX shelf in which it is installed.	45
PATHMA	One or more cross-connected STS or VT1 paths are OOS-MA-AS (Memory Admin.).	49
PROGVER	Program version error. The NEP is running a program version that is not on the COA program backup.	51
PWRF-48VA	Power distribution of −48 Vdc on Side A has failed. A blown shelf fuse could also result in this alarm.	60
PWRF-48VB	Power distribution of −48 Vdc on Side B has failed. A blown shelf fuse could also result in this alarm.	60
SECU-INTRU	A security intrusion alarm has been detected	68
SYNCMA	The NESYNC and/or BITSSYNC synchronization list is OOS-MA (Memory Admin).	81
Condition	**Description**	**Action**
ACOACT	Alarm cutoff – Active	No action
ACODELD	Alarm cutoff – Delayed	No action
ACOIMED	Alarm cutoff – Immediate	No action
ACOMAN	Alarm cutoff – Manual	No action
ADM	NE type – Add-drop multiplexer	No action
INHMSG	All autonomous messages inhibited	No action
INHMSG-CR	Critical autonomous messages inhibited	No action
INHMSG-MJ	Major autonomous messages inhibited	No action
INHMSG-MN	Minor autonomous messages inhibited	No action
INHMSG-NA	Not alarmed autonomous messages inhibited	No action
LINEAR	NE supports line operation only	No action
RING	NE supports line and ring operation	No action
SWDL	Software download in progress	No action

Table A. Common NE Alarms/Conditions/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
TM	NE type: Terminal multiplexer	No action
UPSR-DG1	Some UPSR paths are on DG1	No action
UPSR-DG2	Some UPSR paths are on DG2	No action
UPSR-DG3	Some UPSR paths are on DG3	No action
UPSR-DG4	Some UPSR paths are on DG4	No action
UPSR-DG1A	Some UPSR paths are on DG1A	No action
UPSR-DG2A	Some UPSR paths are on DG2A	No action
UPSR-DG3A	Some UPSR paths are on DG3A	No action
UPSR-DG4A	Some UPSR paths are on DG4A	No action
UPSR-DG1B	Some UPSR paths are on DG1B	No action
UPSR-DG2B	Some UPSR paths are on DG2B	No action
UPSR-DG3B	Some UPSR paths are on DG3B	No action
UPSR-DG4B	Some UPSR paths are on DG4B	No action
UPSR-LG1	Some UPSR paths are on LG1	No action
UPSR-LG2	Some UPSR paths are on LG2	No action
VTGRP	VT1/T1 grouped numbering enabled	No action
VTSEQ	VT1/T1 sequential numbering enabled	No action
Event	**Description**	**Action**
ALMLVL-CR	Alarm level is critical	No action
ALMLVL-MJ	Alarm level is major	No action
ALMLVL-MN	Alarm level is minor	No action
ALMLVL-CL	Alarm level is clear	No action
BUFROVLD	Session overload	*
CAMRBUFROVFL	CAMR buffer overflow	*
OSDRPMSG	OS gateway has dropped a message	No action
PROCROVLD	Processor overload	*
PROGCHK	Flash disk corrupt (read access attempt fails)	No action
RMTDL	Remote download transfer in progress (reported by client NE)	No action
RMTDLFAIL	Remote download failed (reported by client NE)	No action
* *Troubleshoot alarms per TAP-001*		

Alarm/Condition – ALMSYNC

4 Retrieve conditions and determine unit(s) that is reporting ALMSYNC alarm [DLP-100].

5 Place unit reporting ALMSYNC alarm in-service [DLP-501].

6 STOP. This procedure is complete.

Alarm/Condition – BAFFLEALM1 or BAFFLEALM2

7 **NOTE:** *These alarms pertain to the baffle trap doors. Two cables hold the baffle trap doors open. If one of the cables fails, either a BAFFLEALM1 or BAFFLEALM2 alarm is reported. If both cables fail and the baffle trap doors close, both alarms are reported.*

If both alarms are reported, respond immediately at the equipment site.

8 STOP. This procedure is complete.

Alarm/Condition – CONFIG

9 Retrieve provisioned data for an equipment type [DLP-502] and check for a mismatch of provisioned data between Side A and Side B. For example, Side A is provisioned for an HIFB01 and Side B is provisioned for an HIFF01.

NOTE: *For optical LIF units (i.e., LIF401, LIFA01, LIFG01, and LIFF01), Side A and Side B do not have to match if the LIFs are provisioned in SIMPLEX mode.*

10 Was there a mismatch between Side A and Side B of the equipment type?

If yes, go to step 12.
If no, go to step 11.

11 Have all equipment types been checked?

If yes, STOP. This procedure is complete.
If no, return to step 9 and select another equipment type.

12 Is the unit supposed to be equipped?

If yes, go to step 15.
If no, go to step 13.

13 Unassign/delete the unused unit (refer to IXL-001 for appropriate procedure).

14 STOP. This procedure is complete.

15 Remove the incorrect unit and install the correct unit per DLP-101.

16 STOP. This procedure is complete.

Alarm/Condition – EQPTMA

17 Retrieve common alarms and determine which unit(s) is (are) reporting EQPTMA alarm [DLP-100].

18 ***NOTE:*** *In order for entity alarms to be reported, all units should be placed in-service.*

Place unit reporting EQPTMA in-service [DLP-501].

19 STOP. This procedure is complete.

Alarm/Condition – FACMA

20 ***NOTE:*** *If there are several alarmed entities, the Active Conditions listing may be only a partial list of the entities that are Service State = Memory Admin (OOS-MA).*

Retrieve common alarms and determine which facility or facilities is (are) reporting FACMA alarm [DLP-100].

21 Place facility that is reporting FACMA alarm in-service [DLP-501].

22 STOP. This procedure is complete.

Alarm/Condition – FA

23 Locate and check shelf fuses. (See Figure 1).

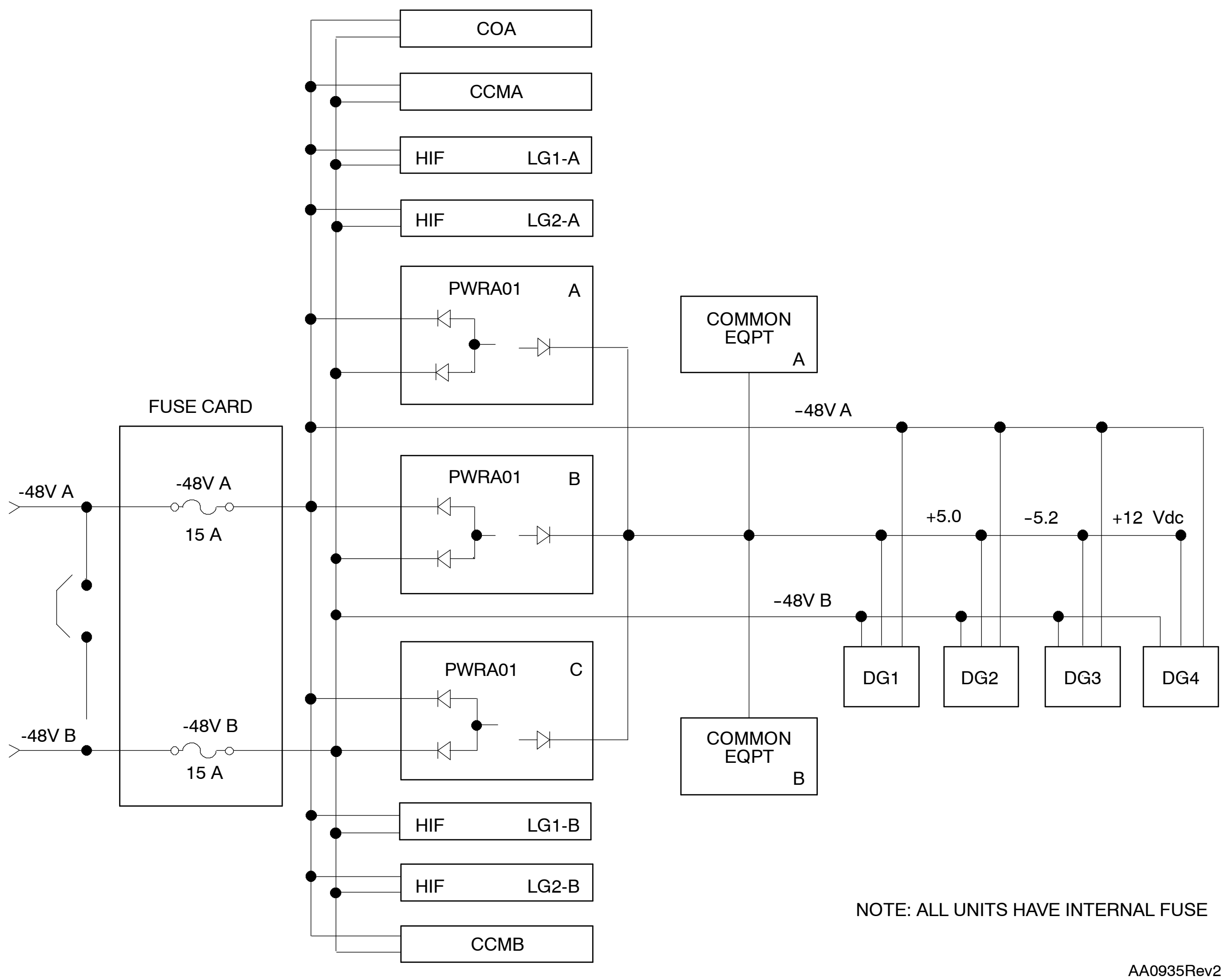


Figure 1. 1603 SMX Shelf Power Distribution

24 Remove the blown fuse and identify amperage or color on indicator.

NOTE: *Fuse should be GMT-10 with Red/White indicator.*

25 Replace blown fuse with good GMT-10 fuse.

26 Did replacement fuse blow?

If yes, go to step 27.
If no, STOP. This procedure is complete.

27 Check shelf backplane for shorted pins, etc.

28 If no shorts are found, review shelf power distribution diagram (Figure 1). Note that PWR units are the only plug-in units that directly use -48 Vdc power.

29 Retrieve alarms [DLP-100].

30 Are there any PWR alarms?

If yes, go to TAP-021.
If no, go to step 31.

31 Contact Alcatel Customer Service for assistance.

32 STOP. This procedure is complete.

Alarm/Condition – FANALM

33 ***NOTE:*** *This condition is externally detected by thermostats wired to the FAN alarm input on the 1603 SMX shelf I/O panel.*

Go to TAP-024 to clear fan alarm.

34 STOP. This procedure is complete.

Alarm/Condition – INVERR

35 Replace NEP per DLP-101.

36 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 37.

37 Suspect backplane Fuse Alarm Unit (FAU). Contact Alcatel Customer Service for assistance.

38 STOP. This procedure is complete.

Alarm/Condition – LOGBUFR90-SECURITY and LOGBUFROVFL-SECURITY

39 ***NOTE:*** *When security log buffer overflow occurs, the oldest messages in the buffer are deleted as new messages are recorded. These alarms can be silenced by initializing the security log; however, initializing the log erases all data in the buffer.*

Do you want to initialize buffer?

If yes, go to step 40.
If no, STOP. This procedure is complete.

40 Initialize security log [DLP-528].

41 STOP. This procedure is complete.

Alarm/Condition – LOGBUFR90-SYSTEM and LOGBUFROVFL-SYSTEM

42 ***NOTE:*** *When system log buffer overflow occurs, the oldest messages in the buffer are deleted as new messages are recorded. These alarms can be silenced by initializing the system log; however, initializing the log erases all data in the buffer.*

Do you want to initialize buffer?

If yes, go to step 43.
If no, STOP. This procedure is complete.

43 Initialize the Alarm/Event Messages log buffer [DLP-528].

44 STOP. This procedure is complete.

Alarm/Condition – MEA

45 ***NOTE:*** *This alarm is for future shelf enhancements that may require software upgrades.*

Replace NEP per DLP-101.

46 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to to step 47.

47 Contact Alcatel Customer Service for assistance.

48 STOP. This procedure is complete.

Alarm/Condition – PATHMA

49 ***NOTE:*** *Entity alarms are not reported unless all cross-connected paths are placed in-service. If there are several alarmed facilities, the Active Conditions listing may be only a partial list of the facilities that are OOS-MA (Memory Admin).*

Determine which paths are in Memory Administration state (OOS-MA); then place these paths in-service [DLP-501].

NOTE: *The parent STS path of a cross-connected VT1.5 path must also be placed in-service.*

50 STOP. This procedure is complete.

Alarm/Condition – PROGVER

51 ***NOTE:*** *You can either silence the alarm, or download the software version that the NEP is running to the COA. COAs 607 - 608 can store up to two versions of complete system software.*

Do you want program backup operational?

If no, go to step 52.
If yes, go to step 54.

52 Change PROGVER notification code to NA (Not Alarmed) [DLP-534].

53 STOP. This procedure is complete.

54 Download software to COA to silence alarm.

NOTE: *To download locally, you must have 1603 SMX Program kit with same version as NEP. To download remotely, a source NE must be available in the SONET network that has the desired software version in its program backup.*

55 Do you want to download locally or remotely?

If locally, go to step 56.
If remotely, go to step 58.

56 Connect PC to craft port (USI) on front of COA [DLP-567] and download software to COA [DLP-570].

57 STOP. This procedure is complete.

58 Remotely download software from another NE [DLP-569].

NOTE: *Green LED flashes on NEP unit at both NEs (server and client) during the download process. Download is completed when LEDs stop flashing.*

59 STOP. This procedure is complete.

Alarm/Condition – PWRF-48VA and PWRF-48VB

60 Is shelf fuse missing?

If yes, replace fuse.
If no, go to step 61.

61 Check for blown fuse on Fuse and Alarm Panel (FAP), if provided, or external power converter. Replace with same size fuse if blown.

62 If fuse blows again, check -48 Vdc wiring to 1603 SMX shelf.

63 Check -48 Vdc distribution fuse panel or circuit breaker panel. Repair per company procedure.

64 If no blown fuses or open circuit breakers are found, measure -48 Vdc power at shelf backplane. Check power connections at shelf.

65 Was cause for alarm found and cleared?

If yes, STOP. This procedure is complete.
If no, go to step 66.

66 Contact Alcatel Customer Service.

67 STOP. This procedure is complete.

Alarm/Condition – SECU-INTRU

68 ***NOTE:*** *A security intrusion condition has been detected and the user interface has been locked. You will not be able to log on using the locked user interface until the specified duration period elapses.*

Are you the system administrator?

If yes, go to step 71.
If no, go to step 69.

69 Contact your system administrator immediately so the security log buffer can be interpreted before the intrusion entry is over-written.

70 STOP. This procedure is complete.

71 ***NOTE:*** *If the intrusion occurred on either of the local user interfaces, both user interfaces are locked. If the intrusion occurred on any of the remote logon sessions, all three remote logon sessions are locked.*

Determine whether to log on to the NE using either local (craft) user interface or one of the three remote logon sessions.

72 Can you log on to the NE using the selected method?

If yes, go to step 74.
If no, go to step 73.

73 Try logging on to the NE using the alternative method.

74 Retrieve the security log [DLP-528] and identify the user interface that has an active lock state and note the UID (username).

75 Contact the appropriate user.

76 Is the user authorized to log on to the NE?

If yes, go to step 77.
If no, go to step 79.

77 Supervisor should evaluate any problems the user is having so this situation can be avoided.

78 STOP. This procedure is complete.

79 Illegal intruder suspected; take appropriate measures per local practice.

80 STOP. This procedure is complete.

Alarm/Condition – SYNCMA

81 ***NOTE:*** *Entity alarms are not reported unless the synchronization list(s) are placed in-service.*

Retrieve service state of NESYNC synchronization reference list [DLP-501].

82 Is Memory Administration current service state of NE Sync?

If yes, go to step 83.
If no, go to step 84.

83 Place NE Sync in-service [DLP-501].

84 Retrieve service state of BITSSYNC synchronization reference list [DLP-501].

85 Is Memory Administration current service state of BITS Sync?

If yes, go to step 86.
If no, go to step 87.

86 Place BITS Sync in-service [DLP-501].

87 STOP. This procedure is complete.

TAP-017
Clear Port Alarm

Purpose

Provides a procedure for clearing a port alarm.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Connect PC to craft port (USI) on front of COA [DLP-567], unless you are logging on to NE remotely.
2	Is the PC communicating with the NE? If yes, go to step 3. If no, go to TAP-039.
3	Are you logged on to the alarmed NE? If yes, then go to step 4. If no, then log on [DLP-117].
4	Have alarms been retrieved for port? If yes, go to step 6. If no, go to step 5.
5	Retrieve alarms [DLP-100].
6	Which port is generating the alarm? If Craft 1, go to step 7. If Craft 2/X.25 (RS-232), go to step 20. If SE2A, go to step 40. If PPP, go to step 48.

Craft 1

7 Check provisioning of Craft 1 port [DLP-502]. Using Table A, analyze the port parameter settings.

8 Note the terminal equipment settings.

9 Are the system parameter settings and terminal settings compatible?

If yes, then go to step 10.
If no, then go to step 12.

10 Suspect a faulty COA or NEP plug-in unit. Go to TAP-021 and check for COA or NEP alarms.

11 STOP. This procedure is complete.

12 Do you need to modify parameters on the port or on the terminal?

If port, then go to step 13.
If terminal, then go to step 18.

13 Modify the required parameters [DLP-502].

14 Retrieve port alarms [DLP-100].

15 Did the alarm condition clear?

If yes, STOP. This procedure is complete.
If no, go to step 16.

16 Suspect a faulty COA or NEP plug-in unit. Go to TAP-021 and check for COA or NEP alarms.

17 STOP. This procedure is complete.

18 Change the terminal parameters so they agree with the port parameters (refer to Tables B and C); then go to step 14.

19 STOP. This procedure is complete.

Table A. RS232 Port Parameters

PORT PARAMETERS	DESCRIPTION
Service State	Used to apply a specific service state on the specified craft port. The parameter can be one of the following: In-Service (IS) Memory Admin (OOS-MA-AS) Unassigned (OOS-MA-UAS)
Stop Bits	Time interval between transmitted characters. Expressed as the number of stop BITS for the craft interface. The parameter value must be 1, 1.5, or 2.
Baud Rate	Data transfer speed for the craft interface. The parameter value can be 1200, 2400, 4800, 9600, 19200, or Autobaud.
Data Bits	Number of data bits sent in each data packet. Referred to as the character size for the craft interface. The parameter value must be 7 or 8 (bits).
Parity	Self-checking method of minimizing transmission errors in transmit and receive data signals. The parameter value must be: NONE (no parity check), ODD (odd parity check), or EVEN (even parity check).
Terminal type	Type of terminal connected to the craft interface. The parameter type must be a VT100 (DEC VT100 compatible device) or a TTY (a hard copy device).
Line Width	Character line width for the craft interface. Any lines with more than the specified line width automatically wrap to the next line on the screen. The parameter must be a value between 10 and 132, inclusive.
Echo	Allows the user to see the outgoing data (keystrokes) on screen when communicating with a remote system. The parameters are: Echo on (full duplex) or echo off (half duplex). Half duplex cannot echo keystrokes to the screen; full duplex can (preferred mode). The value must be Y or N (Y = on, N = off).
XON/XOFF Flow Control	Enables or disables XON/XOFF flow control for Craft 1 and Craft 2 port. The parameter should be Enabled for use with 1301 NMX.

Table B. Communications Port Settings Screen Description

FIELD	MEANING	RANGE/CHOICE
Symbol Label	Displays label applied to communications port	Entered data
Port	Specifies communications port being configured	Com 1 through Com 16*
Baud	Specifies baud rate for port	Recommended rate for modem connection is 9600
Data Format	Three-character format. First character specifies parity for communications port, second character specifies number of bits in a data character, third character specifies number of stop bits used	N-8-1 O-7-1 E-7-1 N-7-21301 NMX-1603 SMX default configuration is N-8-1
OK	Applies specified changes and closes the screen	As shown on screen
Cancel	Closes the screen without applying changes	As shown on screen
Help	Accesses 1301 NMX online help for 1603 SMX applications	As shown on screen
* *Default is COM1.*		

Table C. Modem Port Setup Screen Description

FIELD	MEANING	RANGE/CHOICE
Symbol Label	Displays label applied to the Modem Port icon (If Modem Setup: Phone number is entered, same number is label.)	String of alphanumeric characters
Port	Specifies PCs com port being configured for modem to use	Com1 (default) through Com16
Baud	Specifies baud rate for the port. Set this value to match the network element	1200, 2400, 4800 9600 (Recommended) 14400, 19200 (default) 28800, 38400, 57600 115200
Format	Three-character format. Parity - Data Bits - Stop Bits. Set this value to match the network element	N-8-1 (default) (Recommended) O-7-1 E-7-1 N-7-2
Phone Number	Specifies modem number to be dialed for NE access	Entered data
Timeout	Specifies length of time (in seconds) modem allows to dial and make connection; if no connection within this time, modem hangs up	30—600 seconds 60 (default) (Recommended)
Show terminal after connect (optional)	If selected, allows user interaction after connecting with the remote modem but prior to establishing a connection with the target NE. Used for password entry or call-back modem operation	Selected/Unselected
Modem Init (Optional)	Commands to configure modem before dialing	Hayes-compatible modem command set
Dial Suffix (Optional)	Commands to configure modem after connection has been made	As appropriate per application
OK	Applies the specified changes and closes the setup dialog box	As shown on the screen
Cancel	Closes the window without applying the changes	As shown on the screen
Help	Accesses 1301 NMX online help for 1603 SMX applications	As shown on the screen

Craft 2/X.25

20 Is the COA plug-in unit an odd-numbered COA (two craft ports)?

If yes, go to step 23.
If no, go to step 21.

21 ***NOTE:*** *Craft 2 port (RS-232) is only supported if an odd-numbered COA plug-in unit is installed (i.e., COA601, 603, 605, etc.).*

Replace plug-in unit with correct type per DLP-101.

22 STOP. This procedure is complete.

23 Verify cable connections on the rear of the 1603 SMX shelf. See Figure 1 and DLP-553 for Craft 2 port connections or DLP-019 for X.25 wiring.

24 Are connections correct?

If yes, go to step 27.
If no, go to step 25.

25 Resolve cable connection problem or suspect terminal.

26 STOP. This procedure is complete.

27 Check provisioning of RS232 port [DLP-502]. Using Table A, analyze the port parameter settings.

28 Note the terminal equipment settings.

29 Are the system parameter settings and the terminal settings compatible?

If yes, go to step 30.
If no, go to step 32.

30 Suspect a faulty COA or NEP plug-in unit. Go to TAP-021 and check for COA or NEP alarms.

31 STOP. This procedure is complete.

32 Do you need to modify parameters on the port or on the terminal?

If port, go to step 33.
If terminal, go to step 38.

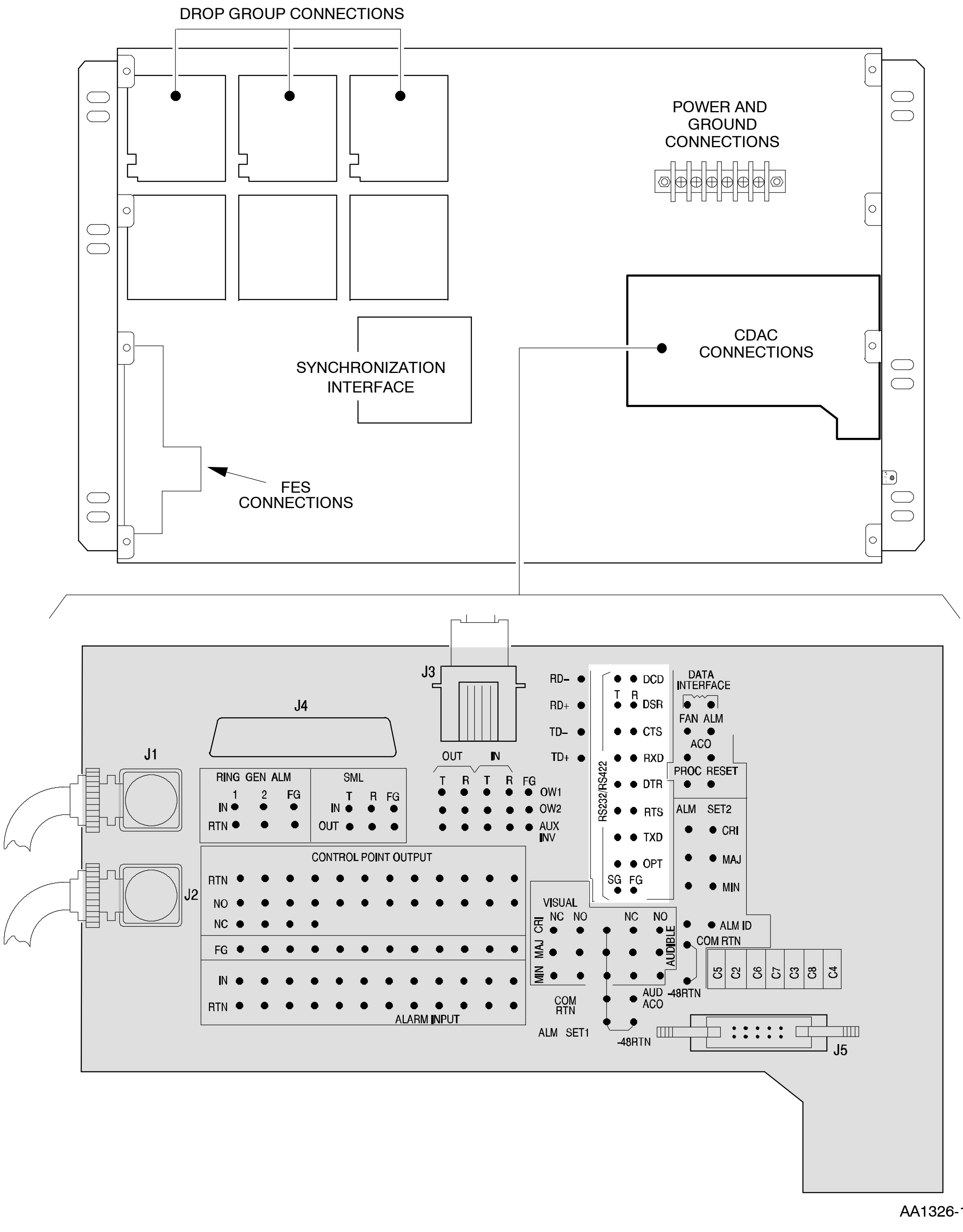


Figure 1. 1603 SMX Shelf, Rear View of Craft 2/E2A Connection Points

33 Modify the required parameters [DLP-502].

34 Retrieve port alarms [DLP-100].

35 Did the alarm condition clear?

If yes, STOP. This procedure is complete.
If no, go to step 36.

36 Suspect a faulty COA or NEP plug-in unit. Go to TAP-021 and check for COA or NEP alarms.

37 STOP. This procedure is complete.

38 Change the terminal parameters so they agree with the port parameters (refer to Tables B and C); then go to step 34.

39 STOP. This procedure is complete.

SE2A

40 Is the COA plug-in unit an even-numbered COA?

If yes, go to step 43.
If no, go to step 41.

41 ***NOTE:*** *SE2A (RS-422) is only supported if an even-numbered COA plug-in unit is installed (i.e., COA602, 604, 606, etc.).*

Replace plug-in unit with correct type per DLP-101.

42 STOP. This procedure is complete.

43 Verify cable connections on the rear of the 1603 SMX shelf. See Figure 1 and DLP-553.

44 Are connections correct?

If yes, go to step 46.
If no, go to step 45.

45 Resolve cable connection problem or suspect terminal.

46 Contact Customer Service.

47 STOP. This procedure is complete.

PPP

48 Is the COA plug-in unit an odd-numbered COA?

If yes, then go to step 51.
If no, then go to step 49.

49 ***NOTE:*** *PPP is only supported if an odd-numbered COA plug-in unit is installed (i.e., COA601, COA603, COA605, etc.).*

Replace plug-in unit with correct type per DLP-101.

50 STOP. This procedure is complete.

51 Retrieve PPP port parameters [DLP-502] and check provisioned values (refer to Table D).

Table D. PPP Port Parameters

PARAMETERS	DESCRIPTION
Service State	Used to apply a specific service state on the specified craft port. The parameter can be one of the following: In-Service (IS), Memory Admin (OOS-MA-AS), or Unassigned (OOS-MA-UAS)
Baud Rate	Data transfer speed for the PPP interface. The parameter value can be 19200 (default), 38400, or 57600
Internet Protocol Address	Entered in dotted decimal notation (ddd.ddd.ddd.ddd). 7..15 alphanumeric characters (quotes are not allowed). Addresses beginning with 127 or 224 through 255 are not allowed and an address of all zeroes is not allowed.
Password Authentication Protocol	Yes (default) or No
Routing Protocol	Routing configuration parameter. Parameter values are OSPF, RIPV1 (RIP Version 1), RIPV2 (RIP Version 2), or No Routing Protocol (default)
OSPF Hello Interval (sec)	Valid values are 1 - 255. (default - 30)
OSPF Router Dead Interval (sec)	Valid values are 1 - 255. (default - 120)
OSPF Retransmission Interval (sec)	Valid values are 1 - 255. (default - 15)
Modem AT Command	0...20 characters (quotes are optional). A null string means send AT only. A nonnull string is appended to AT. (AT is default)

52 Is PPP port provisioned correctly?

If yes, then go to step 55.
If no, go to step 53.

53 Change incorrect parameter(s); then retrieve port alarms [DLP-100].

54 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 55.

55 Check PC setup (refer to Table E).

NOTE: *For more information on setting up the PC to support PPP, refer to the 1603 SMX Provisioning Guide.*

Table E. PC Setup

PARAMETERS	SELECTIONS
Software Compression	Turn off
Password	Do not require an encrypted password
Data Encryption	Do not require encryption data
Network Protocol	Select TCP/IP as an allowed network protocol. TCP/IP is the only protocol that the 1603 SMX will run.
IP Address	The IP address must be specified. The NE will not assign the IP address.
IP Header Compression	Do not use header compression
Default Gateway on Remote Network	If the only network connection is the PPP port, then this parameter should be enabled.

56 Is PC set up correctly to support PPP?

If yes, then go to step 59.
If no, go to step 57.

57 Make necessary changes (refer to Provisioning Guide); then retrieve port alarms [DLP-100].

58 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 59.

59 Check modem port setup (refer to Table C).

60 Is modem port setup correctly?

If yes, then go to step 63.
If no, then go to step 61.

61 Make corrections to the modem port setup; then retrieve port alarms [DLP-100].

62 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 63.

63 Contact Customer Service.

64 STOP. This procedure is complete.

TAP-018
Clear Network Alarm

Purpose

Provides procedures for clearing network alarms.

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

STEP	PROCEDURE
1	Retrieve all active alarms and determine if the NETWORK alarm is a connection (CONN) alarm [DLP-100].
2	Is there a connection (CDACCONN, E2ACONN, or RADCONN) alarm? If yes, go to step 3. If no, go to step 14.
3	Are there any equipment alarms? If yes, go to step 4. If no, go to step 7.
4	***NOTE:*** *All unit alarms are indicated on the COA unit by severity level (CR [Critical], MJ [Major], or MN [Minor]). If there is a COA CONTCOM and an NEP alarm, resolve the COA alarm first.* Identify the alarmed unit with the highest severity.
5	Go to TAP-021 to clear equipment alarms.
6	STOP. This procedure is complete.
7	Are there any OCn or SML facility alarms? If OCn facility alarms, go to TAP-029. If SML facility alarms, go to TAP-033 If there are no facility alarms, go to step 8.

8 **NOTE:** *Both ends of the LLSDCC and LLSMLDCC link must be in-service (pst=IS-NR) for EOC communications to be operational. If one end of the link is OOS-MA-UAS, OOS-MA-AS, or provisioned incorrectly, an EOC alarm is reported at the IS-NR end of the link.*

Are there any lower layer link alarms?

If yes, refer to Table A.
If no, go to step 9.

Table A. Procedures for Clearing Lower Layer Link Alarms

IF LINK REPORTING ALARM IS...	THEN GO TO...
LLSDCC	TAP-032
LLSMLDCC	TAP-045
LAN	TAP-044

9 Retrieve all direct point-to-point neighbors and determine if a lower layer link is not communicating [DLP-560].

10 Determine if there is an NE listed for line group 1, line group 2, and for MAINT1. Any link not listed in the table is a link that is not communicating.

11 Is there a link that is not communicating?

If yes, go to step 12.
If no, go to step 14.

12 Verify operations channel provisioning at local and neighboring NEs [DLP-128].

13 STOP. This procedure is complete.

14 From the response in step 1, select the alarm condition type (refer to Table B) and go to the referenced step.

15 STOP. This procedure is complete.

Table B. Condition Types

CONDITION CODE (CONDNET)	REASON FOR ALARM	STEP
CDACCONN	CDAC connection failure. An external alarm input or control output entry has been made at one NE, but no CDAC connections exist to the remote NE.	16
CDACPROV	CDAC provisioning error. This alarm occurs if one or more CDAC connections already exist between two NEs and an improper entry is made at one of the NEs.	16
E2ACONN	E2A gateway connection failure has occurred between the concentrator and remote NE. The most likely cause of this alarm is a provisioning error at one or both NEs.	24
RADCONN	Communication has not been established between two NEs for Centralized Autonomous Message Reporting (CAMR). Cause could be a connection break or a provisioning error.	34
RADPROV	An NE that is provisioned as a CAMR and FEA concentrator is receiving data from another NE that has also been provisioned as a CAMR/FEA concentrator. Only one CAMR/FEA concentrator is allowed in a network.	34

Alarm/Condition – CDACCONN or CDACPROV

16 At alarmed NE, retrieve provisioned data for NE environmental alarms and controls and check for provisioning errors [DLP-552].

17 Were any problems found at alarmed NE?

If yes, then go to step 20.
If no, then log on to remote NE (netid) and check for provisioning errors.

18 Compare the provisioned data from alarmed NE and remote NE to ensure that each ENV and CONT entry has a corresponding entry for the other NE.

19 Are there any provisioning errors?

If yes, go to step 20.
If no, go to step 22.

20 Correct provisioning errors [DLP-552].

21 Did correcting CDAC provisioning clear alarm?

If yes, STOP. This procedure is complete.
If no, go to step 22.

22 All probable causes have been considered. Look for other (obscure) alarm conditions that may indirectly be causing this alarm [TAP-001] or contact Customer Service.

23 STOP. This procedure is complete.

Alarm/Condition – E2ACONN

24 Retrieve E2A Map provisioning data at the local NE [DLP-561].

25 Is the remote NE name provisioned in the local NE E2A Map?

If yes, go to step 27.
If no, go to step 26.

26 Add remote NE name to local NE E2A Map [DLP-561].

27 Log on to remote NE (netid) and retrieve E2A Map provisioning data at remote NE [DLP-561].

28 Is the local NE name provisioned in the remote NE E2A Map?

If yes, go to step 32.
If no, go to step 29.

29 Add local NE name to remote NE E2A Map [DLP-561].

30 Retrieve alarms at NE with alarm [DLP-100].

31 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 32.

32 All probable causes have been considered. Look for other (obscure) alarm conditions which indirectly may be causing this alarm [TAP-001] or contact Customer Service.

33 STOP. This procedure is complete.

Alarm/Condition – RADCONN or RADPROV

34 Log on to the concentrator NE [DLP-117] and retrieve RADMap provisioning [DLP-562].

35 Log on to remote NE (netid) and retrieve RADMap provisioning [DLP-562].

36 Compare RADMap entries at the local NE and remote NE for inconsistencies.

NOTE: *At the remote NE(s), the NE that is designated as RADMap concentrator should be in the NE Name list. Up to two NEs can be designated as concentrators.*

NOTE: *At the concentrator NE, all the remote NEs that report their autonomous messages to this NE should be listed.*

NOTE: *If two NEs are designated concentrators, only one should be selected for Far End Display.*

NOTE: *The Far End Display Enabled field should be provisioned the same (Yes or No) at both concentrator and remote NEs.*

37 Were inconsistencies found in RADMap provisioning?

If yes, go to step 38.
If no, go to step 40.

38 Correct RADMap entries at remote NE (see step 35) or concentrator NE (see step 34) as required [DLP-562].

39 STOP. This procedure is complete.

40 All probable causes have been considered. Look for other (obscure) alarm conditions that indirectly may be causing this alarm [TAP-001] or contact Customer Service.

41 STOP. This procedure is complete.

TAP-020
Clear ENV Alarm

Purpose

Provides procedure for clearing an environmental (ENV) alarm.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

An ENV alarm indicates that an environmental alarm has been detected on one of the Customer-Defined Alarms and Control (CDAC) alarm inputs on the 1603 SMX backplane.

STEP	PROCEDURE
1	Retrieve customer defined alarms [DLP-100].
2	Note the alarm input (ENV-) number in the Component column and the customer-defined environmental alarm name in the Condition column.
3	Note the severity level (CR, MJ or MN).
4	***NOTE:*** *Resolution of an ENV alarm is typically accomplished by going to the alarmed NE site or by actuating a customer-defined control designed to correct the problem.* Resolve alarm condition per local procedure.
5	STOP. This procedure is complete.

TAP-021
Clear Equipment (EQPT) Alarm

Purpose

Provides procedures for clearing equipment alarms.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Have alarms and conditions been retrieved? If yes, then go to step 3. If no, then continue to step 2.
2	Retrieve alarms [DLP-100].
3	Locate the alarm or condition you want to clear in Table A; then go to the referenced step to clear it. **NOTE:** *Different equipment types can generate the same alarm, so be sure you go to the correct step for the trouble clearing procedure.*

Table A. Equipment Alarms/Conditions/Events

IF ALARM/ CONDITION IS..	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
BKUPMEMP	COA	4	The COA has detected a primary backup memory failure.
BOOT	CCM, DMI, HIF, or LIF	10	Processor in unit reporting this alarm does not have working software installed and is running bootcode only. This alarm is reported if the unit was just installed and an automatic download is in progress. The ACT (green) LED on the alarmed unit flashes during the download process. If a download is in progress, wait until it completes to see if the BOOT alarm clears.
BUERR	CCM	16	A parity error has been detected on an internal STS1 (or GBI) bus between the CCM and interconnecting equipment.
	DMI, HIF, or LIF	29	A parity error has been detected on an internal STS1 bus between the alarmed unit and interconnecting equipment.
	VTG	48	The VTG has experienced a parity error or the VTG bus failed.
CLKFAILTOSW	CCM	59	Clock failed to switch to protection equipment.
CNTBUS	LIF201 or LIF301	66	An error has been detected on the Microprocessor Serial Interface (MSI) bus between an LIF and LDR unit. The alarm is generated by the LIF unit.
	LIF501, LIF601, or LIF701	99	
	LIFD01	124	
CNVT	PWR	162	The power unit converter is in a protective latch-off mode or it has failed. On CCL-B and earlier versions of the PWRA01 power unit, the unit may go into a protection latch-off mode if it detects a fault or momentary low voltage on the incoming -48 Vdc power. The unit will remain in the latch-off mode until it is reseated. Versions CCL-C and later automatically restart when the -48 Vdc input returns to within minimum specified requirements.
CONTBUS	DMI, LIF	174	An error (e.g., loss of frame, reflected parity error, or received parity error) has occurred on the communication bus (SBI) to the NEP.
	HIF	174	The HIF has detected an out-of-frame condition on the communication bus between the unit and the NEP.
	NEP	174	Several things could cause this alarm: the serial bus interface lost its sync, the NEP received a parity error, the TSI loop has failed, or the SML link failed.
	VTG	174	This alarm could be caused by a parity error, a reflection test error, a bus failure, a channel parity error, or a valid interrupt status parity error with the DMI.

Table A. Equipment Alarms/Conditions/Events (cont)

IF ALARM/ CONDITION IS..	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
CONTCOM	CCM, DMI, HIF, or LIF	190	Control Equipment Communications failure. A communication failure has occurred between the active NEP and the unit generating this alarm.
	CLK	209	A communication failure has occurred between the CLK and NEP.
	COA	216	A communication failure has occurred between the COA and NEP
	LDR	222	Reflection test to the controller has failed.
CONTEQPT	DMI, HIF, or LIF	228	Control equipment failure.
	LDR	241	LDR is not reading the control logic.
	NEP	255	An A/B SML select mechanism has failed.
CONTRDUP	CCM, DMI, HIF, or LIF	259	Duplex Control Processor failure. The communication link between an active and standby unit has failed.
CTNEQPT	CCM	269	An interconnection equipment failure has been detected on an internal STS1/GBI bus between the CCM and interconnecting equipment. An LIF/DMI/HIF may be the source of this alarm if the outgoing select status is not echoed back in the received K2 byte.
	DMI, HIF, or LIF	282	An interconnection equipment failure has been detected on an internal STS1 bus between the alarmed unit and interconnecting equipment.
	LDR	302	A Bipolar Data Interface (BDI) data test failure has occurred between an LIF and LDR.
FAILTOSW	CCM, DMI, or LIF	318	Fail to Switch. A unit failed to switch to standby equipment.
	CLK	328	CLK failed to switch to standby equipment.
	LDR	335	LDR failed to switch to standby or protection equipment
	VTG	344	VTG failed to switch to protection equipment.
FWCONTCOM	LIF901	362	A communication failure from the STAR to Ethernet portion of an LIF901 unit has occurred. The most likely cause is an internal board failure.
FWPROGFLT	LIF901	362	A firmware program storage failure has occurred on an LIF901 unit. The most likely cause is an internal board failure.

Table A. Equipment Alarms/Conditions/Events (cont)

IF ALARM/ CONDITION IS..	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
FWMJVER	LIF901	366	The major version number of the firmware image embedded in the system software is different than the major version number of the firmware version currently executing (i.e., the Inuse firmware) on the LAN portion of the LIF901 unit. To clear the alarm, overwrite the Inuse firmware.
FWMNVER	LIF901	371	Firmware minor version error. The minor version number of the firmware image embedded in the system software is different than the minor version number of the Inuse firmware on the Ethernet portion of the LIF901 unit. The system software is compatible with the embedded firmware, but they are at different revision levels.
HITEMP	HIF or LIF	380	An HIF or LIF has detected high laser temperature.
IMPROPRMVL	Any Unit Except NEP	386	Improver Removal. A unit that was not in maintenance state was removed.
INHDGN	Any Unit Except PWR	389	Diagnostics are inhibited on unit generating this alarm.
INHPMREPT	CCM, CLK, DMI, LDR, LIF, or VTG	391	Scheduled PM reporting is inhibited on unit generating this alarm.
INHSWDX	CCM, CLK, DMI, LDR, or LIF	393	Switch to duplex equipment is inhibited on unit generating this alarm.
INHSWPR	LDR, VTG	396	Switch to protection unit is inhibited.
INHSWWKG	LDR, VTG	399	Switch to working unit is inhibited.
INT	CCM, COA, HIF, LDR, LIF, NEP, or VTG	401	An internal hardware failure, such as, an ASIC failure, a read/write check failure, a ASIC identification error, or a device error count failure has occurred on the unit generating the alarm.
	CLK	407	
	DMI	413	
	PWR	162	The power unit converter is in a protective latch-off mode or it has failed.
INVERR	COA	421	Contents of inventory data are inconsistent or absent due to EEPROM communication problem.
	LDR	426	
	VTG	438	
	Any Other Unit	448	
LBCL	HIF or LIF	456	Laser bias threshold failure
LOTEMP	HIF or LIF	380	An HIF or LIF has detected low laser temperature.
LPT	HIF or LIF	380	An HIF or LIF has detected low laser transmit power.

Table A. Equipment Alarms/Conditions/Events (cont)

IF ALARM/ CONDITION IS..	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
MEA	Any Unit	460	Mismatch of Equipment or Attributes
MEMCHK	COA	471	A memory checksum error has been detected on the COA unit.
MEMDIF	COA	477	The COA database (primary) and NEP database (working) are different.
MEMDIFTRAN	COA	482	This alarm typically occurs when an NEP is replaced and it has a different version of software installed than the NE is running. This alarm can also occur after a successful upgrade if the working and primary databases do not match.
MEMVER	COA	488	The COA database (primary) is a different version than the NEP database (working).
MTCE	Any Unit	497	The unit generating the alarm has been removed from service for maintenance.
PLLEOR	CLK	499	The phase lock loop of the clock is reaching its end-of-range.
PROGFLT	CCM, COA, DMI, HIF, or LIF	502	Program storage failure – cannot write to flash memory
PROGVER	CCM,DMI, HIF, or LIF	506	Program Version error. The program version downloaded to the unit generating the alarm is not the same as the NEP version.
PROTNA	LDR501 or VTG	516	Protection is not available for a working LDR501 or VTG unit.
	LIFF01	523	Protection is not available. Mismatched provisioning between A and B LIFF01 facilities.
SWEQPT	VTG	525	The control bus for relays has failed.
SYNC	CCM	544	Unit generating alarm has lost internal shelf clock input.
	HIF or LIF	555	
	NEP	566	
	VTG	584	VTG cannot sync with the incoming (demux) signal or the outgoing (mux) signal.
SYNCCLK	CCM	595	The unit generating the alarm has lost clock synchronization
	CLK	605	
	DMI, HIF, or LIF	617	
	NEP	628	
	VTG	637	

Table A. Equipment Alarms/Conditions/Events (cont)

IF ALARM/ CONDITION IS..	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
SYNCSEL	LIF	647	Synchronization signal failure for NE timing from the LIF. This condition could be due to failure of LIFs in other drop groups.
TRMT	LDR	654	Transmit failure has occurred on an LDR.
Condition	**Action**		**Description**
ACT	No action		Unit is active
AINS	No action		Unit is in Automatic In-Service state
CLKSEL	No action		Selected clock is displayed as comment
CCMCLKSELA	No action		CCM Clock A is clock selected for use by the unit.
CCMCLKSELB	No action		CCM Clock B is clock selected for use by the unit.
STBY	No action		Unit is standby
SWDL	No action		Automatic or manual download in progress
Event	**Action**		**Description**
AINS	No action		Unit is in Automatic In-Service state
AUTODL	No action		Automatic download to in progress
AUTODLFAIL	No action		Automatic download failed
AUTORESET-0	No action		Automatic reset level 0 (warm restart)
AUTORESET-1	No action		Automatic reset level 1 (cold restart)
CTNEQPT	No action		Switch reason: STAR switch
EQUIP	No action		Unit is equipped
FRCDSW	No action		Forced equipment switch
FWAUTODL	No action		Automatic download to FW processor in progress
FWAUTODLFAIL	No action		Automatic download to FW processor failed
FWAUTORESET	No action		Ethernet board processor reset
FWDL	No action		Firmware download in progress, manual or auto
MANRESET-0	No action		Manual reset level 0 (warm restart)
MANRESET-1	No action		Manual reset level 1 (cold restart)
MANRESET-2	No action		Manual reset level 2 (download)
MANSW	No action		Manual equipment switch
UNASSIGN	No action		Unit is unassigned
UNEQUIP	No action		Unit is unequipped
WTRREVERT	No action		Wait to restore timeout (revert)

Alarm/Condition – BKUPMEMP

4 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing COA unit to avoid interrupting service.**

5 Replace the COA unit per DLP-101.

6 Wait for system to initialize; then log on [DLP-117] and retrieve alarms [DLP-100].

7 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 8.

8 Are there any other equipment alarms?

If yes, return to step 3 and clear other alarms.
If no, contact Customer Service.

9 STOP. This procedure is complete.

Alarm/Condition – BOOT

10 Determine download status of NE [DLP-526].

11 Is Automatic S/W Download inhibited?

If yes, then go to step 12.
If no, then go to step 14.

12 Enable the automatic download feature [DLP-527] and wait for auto-download to complete.

13 STOP. This procedure is complete.

14 ***NOTE:*** *If NE is equipped with a COA with expanded memory (COA603 - 610), the COA must have the same version of software that the NEP is running. For software compatibility of units, refer to DLP-101.*

Is the NE equipped with COA with expanded memory or a compatible unit from which software can be auto-downloaded?

If yes, wait for auto-download to complete.
If no, then manually download software from PC to unit [DLP-566].

15 STOP. This procedure is complete.

Alarm/Condition – BUERR (CCM)

16 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

17 Run diagnostic Phase 4 (NSA, STS1 InterConnect test) [DLP-500]. Perform 5 iterations.

18 Did diagnostics pass?

If yes, alarm may be intermittent; go to step 19.
If no, then go to step 21.

19 Continue to monitor for a BUERR alarm and if alarm continues, replace CCM (step 21).

20 STOP. This procedure is complete.

21 Replace alarmed unit per DLP-101; then retrieve alarms [DLP-100].

22 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 23.

23 ***NOTE:*** *The autonomous message, REPT ALM EQPT with an AID of CCM, will most likely include a conddescr parameter. The conddescr parameter identifies the interconnecting plug-in unit that could be causing the alarm.*

Do you have a record of the autonomous message associated with the BUERR alarm?

If yes, then go to step 25.
If no, then continue to step 24.

24 Retrieve alarm history log [DLP-528] and find record of the BUERR alarm.

25 Locate the conddescr parameter found in the autonomous message or alarm history log in Table B. Note the plug-in unit identified by this parameter.

Table B. conddescr Parameters for BUERR Alarm Generated by CCM

CONDDESCR PARAMETERS	PLUG-IN UNIT IDENTIFIED BY PARAMETER
B2ERRORA_1E, _2E, or _3E GBIA_B1ERR_E	Line Group 1, HIF Side A
B2ERRORB_1E, _2E, or _3E GBIB_B1ERR_E	Line Group 1, HIF Side B
B2ERRORA_1W, _2W, or _3W GBIA_B1ERR_W	Line Group 2, HIF Side A
B2ERRORB_1W, _2W, or _3W GBIB_B1ERR_W	Line Group 2, HIF Side B
B2ERRORA_DG1_1, _2, or _3	Drop Group 1, DMI/LIF Side A
B2ERRORB_DG1_1, _2, or _3	Drop Group 1, DMI/LIF Side B
B2ERRORA_DG2_1, _2, or _3	Drop Group 2, DMI/LIF Side A
B2ERRORB_DG2_1, _2, or _3	Drop Group 2, DMI/LIF Side B
B2ERRORA_DG3_1, _2, or _3	Drop Group 3, DMI/LIF Side A
B2ERRORB_DG3_1, _2, or _3	Drop Group 3, DMI/LIF Side B
B2ERRORA_DG4_1, _2, or _3	Drop Group 4, DMI/LIF Side A
B2ERRORB_DG4_1, _2, or _3	Drop Group 4, DMI/LIF Side B

26 Replace plug-in unit per DLP-101 identified in Table B; then retrieve alarms [DLP-100].

27 Did BUERR alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

28 STOP. This procedure is complete.

Alarm/Condition – BUERR (DMI, LIF, or HIF)

29 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

30 Run diagnostic Phase 4 (NSA, STS1 InterConnect test) [DLP-500]. Perform 5 iterations.

31 Did diagnostics pass?

If yes, alarm may be intermittent. Go to step 32.
If no, then go to step 34.

32 Continue to monitor for a BUERR alarm and if alarm continues, replace unit reporting alarm (step 34).

33 STOP. This procedure is complete.

34 Replace alarmed unit per DLP-101; then retrieve alarms [DLP-100].

35 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 36.

36 ***NOTE:*** *The autonomous message, REPT ALM EQPT, with an aid of DGx-DMIy, DGx-LIFy, or LGx-HIFy, will most likely include a conddescr parameter. The conddescr parameter indicates on which side of the STS1 (/GBI) bus (Side A or Side B) the error was detected.*

Do you have a record of autonomous message associated with the BUERR alarm?

If yes, then go to step 38.
If no, then continue to step 37.

37 Retrieve alarm history log [DLP-528] and find record of the BUERR alarm.

38 Does the autonomous record include a conddescr parameter?

If yes, then continue to step 39.
If no, then go to step 43.

39 Locate the conddescr parameter found in the autonomous message or alarm history log in Table C. Note which side of STS1 (/GBI) bus is indicated by conddescr parameter.

Table C. conddescr Parameters for BUERR Alarm Generated by DMI, HIF, or LIF

CONDDESCR PARAMETERS	INTERNAL STS1 BUS SIDE INDICATED BY CONDDESCR
B2ERRORA B2ERRORA_L1, _L2, or _L3 GBIA-B1ERR	Side A
B2ERRORB B2ERRORB_L1, _L2, or _L3 GBIB-B1ERR	Side B

40 Which side of STS1 (/GBI) bus is reporting alarm?

If Side A, replace CCM-A unit per DLP-101; then retrieve alarms.
If Side B, replace CCM-B unit per DLP-101; then retrieve alarms.

41 Did BUERR alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

42 STOP. This procedure is complete.

43 Replace the standby CCM unit per DLP-101; then retrieve alarms [DLP-100].

44 Did BUERR alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 45.

45 Switch the active and standby CCM units and replace the CCM unit that is now in standby; then retrieve alarms [DLP-100].

46 Did BUERR alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

47 STOP. This procedure is complete.

Alarm/Condition – BUERR (VTG)

48 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

49 If you do not know which VTG is generating the alarm, retrieve VTG alarms [DLP-100].

50 Run diagnostic Phase 3 (NSA, Active Reflection) on alarmed VTG and if DMIs are redundant, also run Phase 4 (NSA, Inactive Reflection) [DLP-500]. Perform 5 iterations.

51 Did diagnostics pass?

If yes, go to step 54.
If no, then go to step 52.

52 Replace alarmed unit per DLP-101; then retrieve alarms [DLP-100].

53 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 54.

54 Are there any DMI alarms?

If yes, return to step 3 and clear DMI alarms.
If no, then continue to step 55.

55 **NOTE:** *From the alarm response for the VTG BUERR alarm, the Side column (AIDDET parameter) contains the character A or B, which identifies the DMI (Side A or Side B) serving the alarmed VTG.*

From the response, determine if the fault is detected at the Side-A DMI or Side-B DMI.

56 Replace the DMI identified in step 55 [DLP-101]; then retrieve alarms [DLP-100].

57 Did BUERR alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

58 STOP. This procedure is complete.

Alarm/Condition – CLKFAILTOSW

59 **CAUTION: Possibility of service interruption. Adhere to procedures in DLP-101 when replacing the CCM unit to avoid interrupting service.**

60 Replace standby CCM unit per DLP-101; then retrieve CCM alarms [DLP-100].

61 Did CLKFAILTOSW alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 62.

62 Switch CCMs [DLP-505].

63 Replace CCM unit that was active per DLP-101; then retrieve alarms [DLP-100].

64 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

65 STOP. This procedure is complete.

Alarm/Condition – CNTBUS (LIF201/LIF301)

66 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid service interruption.**

67 Is the unit redundant or non-redundant?

If non-redundant, then continue to step 68.
If no, then go to step 82.

Non-Redundant LIF201/LIF301 Unit

68 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF and LDR units.**

69 Place LIF generating alarm in maintenance state [DLP-501].

70 Run all diagnostic phases on alarmed LIF [DLP-500]. Perform one iteration.

71 Did diagnostics pass?

If yes, then go to step 73.
If no, replace LIF per DLP-101.

72 STOP. This procedure is complete.

73 Place LIF back in-service [DLP-501].

74 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR.**

75 Place LDR associated with alarmed LIF in maintenance state [DLP-501].

76 Run all diagnostic phases on associated LDR [DLP-500]. Perform one iteration.

77 Did diagnostics pass?

If yes, then go to step 79.
If no, replace LDR per DLP-101.

78 STOP. This procedure is complete.

79 Place LDR back in service [DLP-501].

80 Suspect backplane bus problem; contact Customer Service.

81 STOP. This procedure is complete.

Redundant LIF201/LIF301 Unit

82 ***NOTE:*** *The active and standby LIFs will be switched to determine whether the active LIF or active LDR is causing the alarm. When LIF20x units are switched, the LDRs also switch, i.e., LDR-A is active when LIF-A is active, and LDR-B is active when LIF-B is active.*

Switch to redundant LIF [DLP-505]; then retrieve alarms [DLP-100].

83 Did CNTBUS alarm clear (may take several minutes)?

If yes, then go to step 86.
If no, then continue to step 84.

84 Suspect backplane bus problem; contact Customer Service.

85 STOP. This procedure is complete.

86 Problem must be in standby LIF or LDR. Go to step 87 and perform diagnostics on LIF.

87 **CAUTION: Possibility of service interruption. Some diagnostic phases are service-affecting if performed on an active unit. Be sure the LIF and LDR units are in maintenance state before performing diagnostics.**

88 Place LIF generating alarm in maintenance state [DLP-501].

89 Run all diagnostic phases on alarmed LIF [DLP-500]. Perform one iteration.

90 Did diagnostics pass?

If yes, then go to step 92.
If no, replace LIF per DLP-101.

91 STOP. This procedure is complete.

92 Place LIF back in-service [DLP-501].

93 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR. Perform the following on standby side if LIF and LDR are redundant.**

94 Place LDR associated with alarmed LIF in maintenance state [DLP-501].

95 Run all diagnostic phases on associated LDR. Perform one iteration [DLP-500].

96 Did diagnostics pass?

If yes, place LDR back in-service [DLP-501]; then go to step 97.
If no, replace LDR per DLP-101; then go to step 98.

97 Suspect backplane bus problem. Contact Customer Service.

98 STOP. This procedure is complete.

Alarm/Condition – CNTBUS (LIF501/LIF601/701)

99 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid service interruption.**

100 Is the unit redundant or non-redundant?

If non-redundant, then continue to step 101.
If redundant, then go to step 115.

Non-Redundant LIF501/LIF601/LIF701 Unit

101 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF and LDR units.**

102 Place LIF generating alarm in maintenance state [DLP-501].

103 Run all diagnostic phases on alarmed LIF [DLP-500]. Perform one iteration.

104 Did diagnostics pass?

If yes, then go to step 106.
If no, replace LIF per DLP-101.

105 STOP. This procedure is complete.

106 Place LIF back in-service [DLP-501].

107 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR.**

108 Place LDR associated with alarmed LIF in maintenance state [DLP-501].

109 Run all diagnostic phases on associated LDR [DLP-500]. Perform one iteration.

110 Did diagnostics pass?

If yes, then go to step 79.
If no, replace LDR per DLP-101.

111 STOP. This procedure is complete.

112 Place LDR back in service [DLP-501].

113 Suspect backplane bus problem; contact Customer Service.

114 STOP. This procedure is complete.

Redundant LIF501/LIF601/LIF701 Unit

115 ***NOTE:*** *The active and standby LIFs associated with the alarmed facility will be switched to determine whether the active LIF is causing the alarm. If the alarm isn't cleared, the active and standby LDRs associated with the alarmed facility will be switched.*

Switch to redundant LIF [DLP-505]; then retrieve alarms [DLP-100].

116 Did CNTBUS alarm clear (may take several minutes)?

If yes, replace standby LIF per DLP-101.
If no, then go to step 118.

117 STOP. This procedure is complete.

118 Switch to redundant LDR [DLP-505]; then retrieve alarms [DLP-100].

119 Did CNTBUS alarm clear (may take several minutes)?

If yes, replace standby LDR per DLP-101.
If no, then go to step 120.

120 Suspect backplane bus problem. Contact Customer Service.

121 STOP. This procedure is complete.

Alarm/Condition – CNTBUS (LIFD01)

122 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid service interruption.**

123 Is the unit redundant or non-redundant?

If non-redundant, then continue to step 124.
If redundant, then go to step 130.

Non-Redundant LIFD01 Unit

124 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF unit.**

125 Place LIF to be tested in maintenance state [DLP-501].

126 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

127 Did diagnostics pass?

If yes, place LIF back in-service [DLP-501]; then go to step 128.
If no, replace LIF per DLP-101; then go to step 129.

128 Contact Customer Service.

129 STOP. This procedure is complete.

Redundant LIFD01 Unit

130 Switch to redundant LIF [DLP-505]; then retrieve LIF alarms [DLP-100].

131 Did CNTBUS alarm clear (may take several minutes)?

If yes, replace standby LIF per DLP-101.
If no, then go to step 133.

132 STOP. This procedure is complete.

133 Run diagnostic Phases 7 (Local MSI Loopback test) and Phase 8 (Inter LIF-LIF Communications test via MSI Bus) on active LIF [DLP-500]. Perform one iteration.

134 Did Phases 7 and 8 pass?

If yes, contact Customer Service.
If no, refer to Table D.

Table D. LIF Diagnostic Results

IF PHASE 7...	AND PHASE 8...	THEN GO TO...
Passed	Failed	Step 135
Failed	Passed	Step 137
Failed	Failed	Step 139

135 Replace standby LIF per DLP-101.

136 STOP. This procedure is complete.

137 Replace active LIF per DLP-101.

138 STOP. This procedure is complete.

139 Run diagnostic Phase 1 (NSA, LIF/LDR control bus test) on any LDR in either group [DLP-500]. Perform one iteration.

140 Did diagnostics pass?

If yes, replace active LIF per DLP-101; then go to step 141.
If no, then go to step 142.

141 STOP. This procedure is complete.

142 Replace standby LIF per DLP-101.

143 Run diagnostic Phases 7 and 8 on standby LIF [DLP-500]. Perform one iteration.

144 Did diagnostics pass?

If yes, STOP. This procedure is complete.
If no, then continue to step 145.

145 Replace active LIF per DLP-101.

146 Run diagnostic Phases 7 and 8 on active LIF [DLP-500]. Perform one iteration.

147 Did diagnostics pass?

If yes, STOP. This procedure is complete.
If no, then continue to step 148.

148 In LDR Group 1, remove protection LDR (LDR-P) from service [DLP-501]. See Figure 1 for LDR501 locations.

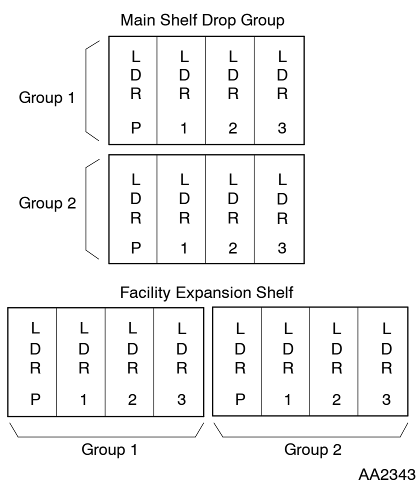


Figure 1. LDR501 Locations in Main Shelf and Facility Expansion Shelf (FES)

149 Run diagnostic Phases 7 and 8 on active LIF [DLP-500]. Perform one iteration.

150 Did diagnostics pass?

If yes, then go to step 152.
If no, return protection LDR to service; then continue to step 151.

151 Has protection LDR been removed from LDR Group 2?

If yes, then go to step 154.
If no, remove protection LDR from Group 2; then go to step 149.

152 Replace LDR that was removed from service [DLP-101].

153 STOP. This procedure is complete.

154 In LDR Group 1, switch a working LDR to protection [DLP-529].

155 Remove working LDR that was switched to protection from service [DLP-501].

156 Run diagnostic Phases 7 and 8 on active LIF [DLP-500]. Perform one iteration.

157 Did diagnostics pass?

If yes, then replace LDR that was removed from service [DLP-101].
If no, return LDR to service [DLP-501]; then go to step 159.

158 STOP. This procedure is complete.

159 Have all LDRs in Group 1 and 2 been removed from service?

If yes, then continue to step 160.
If no, select a different LDR and repeat from step 154.

160 Suspect backplane bus problems. Contact Customer Service.

161 STOP. This procedure is complete.

Alarm/Condition – CNVT or PWR Generated INT

162 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid interrupting service.**

163 ***NOTE:*** *On CCL-B and earlier versions of the PWRA01 power unit, the unit may go into a protection latch-off mode if it detects a fault or momentary low voltage on the incoming -48 Vdc power. The unit remains in the latch-off mode until it is reseated. Versions CCL-C and later automatically restart when the -48 Vdc input returns to within minimum specified requirements.*

Is the alarmed PWRA01 power unit version CCL-B (or earlier) or CCL-C (or later)?

If CCL-B (or earlier), then continue to step 164
If CCL-C (or later), then go to step 165.

164 Remove the unit and inspect for signs of physical damage.

If no damage was found, reinstall the PWR unit; then go to step 166.
If damage was found, then continue to step 165.

165 Replace the alarmed PWR unit per DLP-101.

166 Retrieve alarms [DLP-100].

167 Did CNVT alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 168.

168 Do any units have an ALM LED lighted?

If yes, replace the unit with the lighted LED [DLP-101].
If no, then go to step 170.

169 STOP. This procedure is complete.

170 ***NOTE:*** *Either there is a short on a power bus or a unit is overloading.*

See Figure 1 for shelf power distribution diagram.

171 Remove inactive (standby) units in the following order until power returns: LDRs/VTGs, DMIs/LIFs, NEP, COA, CLK, CCM, and HIF.

172 Resolve short or replace unit [DLP-101] that is over loading the power supply.

173 STOP. This procedure is complete.

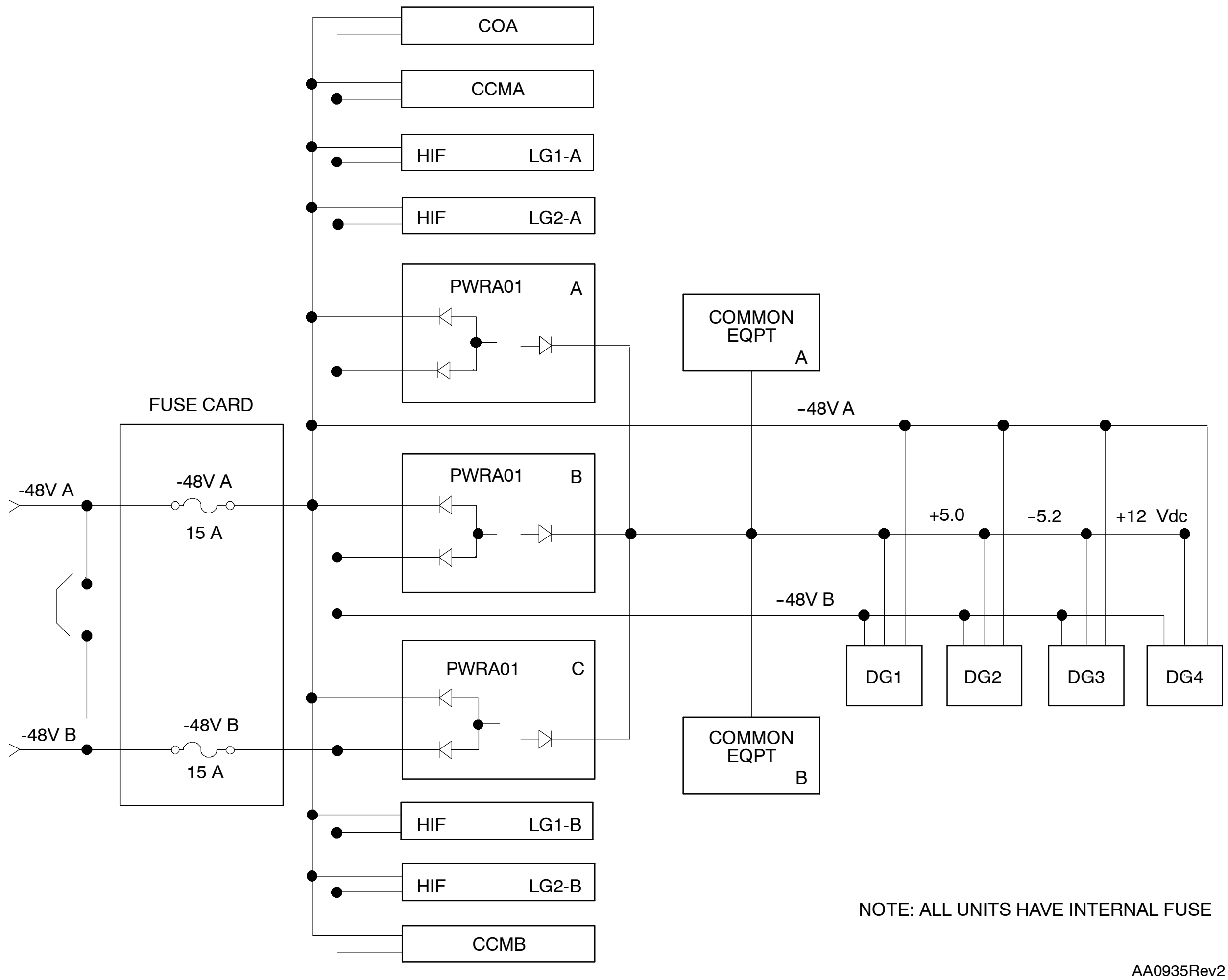


Figure 1. 1603 SMX Shelf Power Distribution

Alarm/Condition – CONTBUS

174 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing plug-in units to avoid interrupting service.**

175 Run diagnostics on unit generating alarm [DLP-500]. Refer to Table E for diagnostic phases to run. Perform 5 iterations.

Table E. Diagnostic Phases to Run for CONTBUS Alarm

IF UNIT GENERATING ALARM IS...	THEN RUN...,
DMI	Phase 1 - NSA, Active NEP-DMI Comm.
HIF	Phase 1 - NSA, Active NEP-HIF Comm.
LIF	Phase 1 - NSA, Active NEP-LIF Comm.
NEP	Phase 2 - NSA, TSI SBI Loop and Phase 10 - NSA, SML Active Reflection

176 Did diagnostic phase pass?

If yes, alarm may be intermittent. Go to step 177.
If no, then go to step 179.

177 Continue to monitor for a CONTBUS alarm. If alarm continues, go to step 179.

178 STOP. This procedure is complete.

179 Replace alarmed unit per DLP-101; then retrieve alarms [DLP-100].

180 Did CONTBUS alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 181.

181 Is alarm being generated by an NEP?

If yes, then continue to step 182.
If no, then go to step 183.

182 Was a CONTCOM alarm being generated by another unit?

If yes, return to step 3 and clear this alarm.
If no, contact Customer Service.

183 Is alarm being generated by a VTG?

If yes, then continue to step 184.
If no, then go to step 188.

184 Are there any DMI alarms?

If yes, return to step 3 and clear DMI alarms.
If no, then continue to step 185.

185 **NOTE:** *From the alarm response for the CONTBUS alarm, the Side column (AIDDET parameter) contains the character A or B, which identifies the DMI (Side A or Side B) serving the alarmed VTG.*

From the response, determine if the fault is detected at the Side-A DMI or Side-B DMI.

186 Replace the DMI identified in step 185 [DLP-101]; then retrieve alarms [DLP-100].

187 Did CONTBUS alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

188 Are there any NEP alarms?

If yes, return to step 3 and clear NEP alarms.
If no, contact Customer Service.

189 STOP. This procedure is complete.

Alarm/Condition – CONTCOM (CCM, DMI, HIF, or LIF)

190 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing plug-in units to avoid interrupting service.**

191 Run diagnostic Phase 1 (NSA, Active NEP to <*unit name*> Communications test) on unit generating alarm [DLP-500]. Perform 5 iterations.

192 Did diagnostics pass?

If yes, alarm may be intermittent. Go to step 193.
If no, then go to step 195.

193 Continue to monitor for a CONTCOM alarm. If alarm continues, go to step 195.

194 STOP. This procedure is complete.

195 Replace alarmed unit per DLP-101; then retrieve alarms [DLP-100].

196 Did CONTCOM alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 197.

197 Replace NEP per DLP-101; then retrieve alarms [DLP-100].

198 Did CONTCOM alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 199.

199 Is CCM unit generating the alarm?

If yes, then go to step 207.
If no, then continue to step 200.

200 Replace same side CCM unit (i.e., if alarmed unit is on Side A , replace CCM-A and if alarmed unit is on Side B, replace CCM-B). Refer to DLP-101.

201 Retrieve alarms [DLP-100].

202 Did CONTCOM alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 203.

203 Replace opposite side CCM unit per DLP-101; then retrieve alarms [DLP-100].

204 Did CONTCOM alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 205.

205 Replace COA unit [DLP-101]; then retrieve alarms [DLP-100].

206 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 207.

207 Suspect backplane bus problem. Contact Customer Service.

208 STOP. This procedure is complete.

Alarm/Condition – CONTCOM (CLK)

209 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing plug-in units to avoid interrupting service.**

210 Run diagnostic Phase 1 (NSA, Active NEP-CLOCK Communication test) on CLK unit [DLP-500]. Perform one iteration.

211 Did diagnostic phase pass?

If yes, then continue to step 212.
If no, then go to step 213.

212 Check for NEP alarms because the NEP is probably processing the wrong message.

213 Replace alarmed clock unit per DLP-101; then retrieve alarms [DLP-100].

214 Did CONTCOM alarm clear?

If yes, STOP. This procedure is complete.
If no, suspect NEP is processing wrong message.

215 STOP. This procedure is complete.

Alarm/Condition – CONTCOM (COA)

216 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing plug-in units to avoid interrupting service.**

217 Replace COA unit per DLP-101.

218 Wait for system to initialize; then log on [DLP-117] and retrieve alarms [DLP-100].

219 Did CONTCOM alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 220.

220 Are there any other equipment alarms?

If yes, return to step 3 and clear other equipment alarms
If no, contact Customer Service.

221 STOP. This procedure is complete.

Alarm/Condition – CONTCOM (LDR)

222 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing plug-in units to avoid interrupting service.**

223 Run diagnostic Phase 1 (NSA, LIF/LDR Control Bus test) on LDR generating alarm [DLP-500]. Perform 5 iterations.

224 Did diagnostics pass?

If yes, suspect a bad active LIF.
If no, then continue to step 225.

225 Replace alarmed LDR per DLP-101; then retrieve alarms [DLP-100].

226 Did CONTCOM alarm clear?

If yes, STOP. This procedure is complete.
If no, suspect a bad active LIF.

227 STOP. This procedure is complete.

Alarm/Condition – CONTEQPT (DMI, HIF, or LIF)

228 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

229 Run diagnostic Phase 3 (NSA, Switch Code test) on alarmed unit [DLP-500]. Perform 5 iterations.

230 Did diagnostics pass?

If yes, alarm may be intermittent. Go to step 231.
If no, then go to step 233.

231 Continue to monitor for CONTCOM alarms. If alarm continues, go to step 233.

232 STOP. This procedure is complete.

233 Replace the alarmed LIF per DLP-101; then retrieve alarms [DLP-100].

234 Did CONTEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 235.

235 Replace the COA per DLP-101; then retrieve alarms [DLP-100].

236 Did CONTEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 237.

237 Replace the NEP per DLP-101; then retrieve alarms [DLP-100].

238 Did CONTEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 239.

239 Suspect backplane bus problem; contact Customer Service.

240 STOP. This procedure is complete.

Alarm/Condition – CONTEQPT (LDR)

241 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

242 Retrieve alarms [DLP-100].

243 Are there any other LDR units generating alarms in the same drop group?

If yes, then go to step 247.
If no, then continue to step 244.

244 Replace the alarmed LDR per DLP-101; then retrieve alarms [DLP-100].

245 Did CONTEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 246.

246 Was standby LIF replaced?

If yes, then go to step 251.
If no, then continue to step 247.

247 Replace the standby LIF per DLP-101.

248 Retrieve alarms [DLP-100].

249 Did CONTEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 250.

250 Was the alarmed LDR replaced?

If yes, then continue to step 251.
If no, then go to step 244.

251 Were both LIFs replaced?

If yes, then go to step 253.
If no, then continue to step 252.

252 Replace the other LIF unit per DLP-101; then go to step 248.

253 Alarm could be caused by a bus problem. Contact Customer Service.

254 STOP. This procedure is complete.

Alarm/Condition – CONTEQPT (NEP)

255 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

256 Replace the NEP per DLP-101; then retrieve alarms [DLP-100].

257 Did CONTEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

258 STOP. This procedure is complete.

Alarm/Condition – CONTRDUP

259 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

260 Run diagnostic Phase 5 (NSA, Inter Unit Communication test) on alarmed unit [DLP-500]. Perform 5 iterations.

261 Did diagnostics pass?

If yes, alarm may be intermittent; go to step 262.
If no, then go to step 264.

262 Continue to monitor for CONTRDUP alarms. If alarm continues, go to step 264.

263 STOP. This procedure is complete.

264 Replace alarmed unit per DLP-101; then retrieve alarms [DLP-100].

265 Did CONTRDUP alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 266.

266 Replace opposite side unit per DLP-101; then retrieve alarms [DLP-100].

267 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, suspect backplane bus problem; contact Customer Service.

268 STOP. This procedure is complete.

Alarm/Condition – CTNEQPT (CCM)

269 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

270 Run diagnostic Phase 4 (NSA, STS1 InterConnect test) on alarmed CCM [DLP-500]. Perform 5 iterations.

271 Did diagnostics pass?

If yes, alarm may be intermittent. Go to step 272.
If no, then go to step 274.

272 Continue to monitor for CTNEQPT alarms. If alarm continues go to step 274.

273 STOP. This procedure is complete.

274 Replace alarmed CCM per DLP-101; then retrieve alarms [DLP-100].

275 Did CTNEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 276.

276 **NOTE:** *The autonomous message, REPT ALM EQPT with an aid of CCM, will most likely include a conddescr parameter. The conddescr parameter identifies the interconnecting plug-in unit that could be causing the alarm.*

Do you have a record of the autonomous message associated with the CTNEQPT alarm?

If yes, then go to step 278.
If no, then continue to step 277.

277 Retrieve alarm history log [DLP-528] and find record of CTNEQPT alarm.

278 Locate the conddescr parameter found in the autonomous message or history log on Table F. Note the plug-in unit identified by this parameter.

279 Replace plug-in unit identified by conddescr parameter [DLP-101]; then retrieve alarms [DLP-100].

280 Did CTNEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

281 STOP. This procedure is complete.

Table F. conddescr Parameters for CTNEQPT Alarm Generated by CCM

CONDDESCR PARAMETERS	PLUG-IN UNIT IDENTIFIED BY PARAMETER
A1A2ERRORA_1E, 2E_, or _3E	Line Group 1, HIF Side A
A1A2ERRORB_1E, 2E_, or _3E	Line Group 1, HIF Side B
A1A2ERRORA_1W, 2W_, or _3W	Line Group 2, HIF Side A
A1A2ERRORB_1W, 2W_, or _3W	Line Group 2, HIF Side B
ESALIGN_1E, _2E, or _3E	Line Group 1, HIF
ESALIGNA_1E, _2E, or _3E	Line Group 1, HIF Side A
ESALIGNB_1E, _2E, or _3E	Line Group 1, HIF Side B
ESALIGN_1W, _2W, or _3W	Line Group 2, HIF
ESALIGNA_1W, _2W, or _3W	Line Group 2, HIF Side A
ESALIGNB_1W, _2W, or _3W	Line Group 2, HIF Side B
GBIAFAIL_E	Line Group 1, HIF Side A
GBIBFAIL_E	Line Group 1, HIF Side B

Table F. conddescr Parameters for CTNEQPT Alarm Generated by CCM (cont)

CONDDESCR PARAMETERS	PLUG-IN UNIT IDENTIFIED BY PARAMETER
GBIAFAIL_W	Line Group 2, HIF Side A
GBIBFAIL_W	Line Group 2, HIF Side B
ISOCTNEQPT	CCM
STSAFAIL_1E, _2E, or _3E	Line Group 1, HIF Side A
STSBFAIL_1E, _2E, or _3E	Line Group 1, HIF Side B
STSAFAIL_1W, _2W, or _3W	Line Group 2, HIF Side A
STSBFAIL_1W, _2W, or _3W	Line Group 2, HIF Side B
STSAFAILSW_1E, _2E, or _3E	Line Group 1, HIF Side A
STSBFAILSW_1E, _2E, or _3E	Line Group 1, HIF Side B
STSAFAILSW_1W, _2W, or _3W	Line Group 2, HIF Side A
STSBFAILSW_1W, _2W, or _3W	Line Group 2, HIF Side B
STSAFAIL_DG1_1, _2, or _3	Drop Group 1, DMI/LIF Side A
STSAFAIL_DG2_1, _2, or _3	Drop Group 2, DMI/LIF Side A
STSAFAIL_DG3_1, _2, or _3	Drop Group 3, DMI/LIF Side A
STSAFAIL_DG4_1, _2, or _3	Drop Group 4, DMI/LIF Side A
STSBFAIL_DG1_1, _2, or _3	Drop Group 1, DMI/LIF Side B
STSBFAIL_DG2_1, _2, or _3	Drop Group 2, DMI/LIF Side B
STSBFAIL_DG3_1, _2, or _3	Drop Group 3, DMI/LIF Side B
STSBFAIL_DG4_1, _2, or _3	Drop Group 4, DMI/LIF Side B
STSAINTERX_GBI_E	Line Group 1, HIF Side A
STSAINTERX_1E, _2E, or _3E	Line Group 1, HIF Side A
STSBINTERX_GBI_E	Line Group 1, HIF Side B
STSBINTERX_1E, _2E, or _3E	Line Group 1, HIF Side B
STSAINTERX_GBI_W	Line Group 2, HIF Side A
STSAINTERX_1W, _2W, or _3W	Line Group 2, HIF Side A
STSBINTERX_GBI_W	Line Group 2, HIF Side B
STSBINTERX_1W, _2W, or _3W	Line Group 2, HIF Side B
STSAINTERX_DG1_1, _2, or _3	Drop Group 1, DMI/LIF Side A

Table F. conddescr Parameters for CTNEQPT Alarm Generated by CCM (cont)

CONDDESCR PARAMETERS	PLUG-IN UNIT IDENTIFIED BY PARAMETER
STSBINTERX_DG1_1, _2, or _3	Drop Group 1, DMI/LIF Side B
STSAINTERX_DG2_1, _2, or _3	Drop Group 2, DMI/LIF Side A
STSBINTERX_DG2_1, _2, or _3	Drop Group 2, DMI/LIF Side B
STSAINTERX_DG3_1, _2, or _3	Drop Group 3, DMI/LIF Side A
STSBINTERX_DG3_1, _2, or _3	Drop Group 3, DMI/LIF Side B
STSAINTERX_DG4_1, _2, or _3	Drop Group 4, DMI/LIF Side A
STSBINTERX_DG4_1, _2, or _3	Drop Group 4, DMI/LIF Side B

Alarm/Condition – CTNEQPT (DMI, HIF, or LIF)

282 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

283 Run diagnostic Phase 4 (NSA, STS1 InterConnect test) on alarmed unit [DLP-500]. Perform 5 iterations.

284 Did diagnostics pass?

If yes, alarm may be intermittent. Go to step 285.
If no, then go to step 287.

285 Continue to monitor for CTNEQPT alarms. If alarm continues go to step 287.

286 STOP. This procedure is complete.

287 Replace alarmed unit per DLP-101; then retrieve alarms [DLP-100].

288 Did CTNEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 289.

289 ***NOTE:*** *The autonomous message, REPT ALM EQPT with an aid of DGx-DMIy, DGx-LIFy, or LGx-HIFy, will most likely include a conddescr parameter. The conddescr parameter indicates on which side of the STS1 (/GBI) bus (Side A or Side B) the error was detected.*

Do you have a record of the autonomous message associated with the CTNEQPT alarm?

If yes, then go to step 291.
If no, then continue to step 290.

290 Retrieve alarm history log [DLP-528] and find record of CTNEQPT alarm.

291 Does the autonomous record include a conddescr parameter?

If yes, then continue to step 292.
If no, then go to step 296.

292 Locate the conddescr parameter found in the autonomous message or history log in Table G. Note the bus side identified by this parameter.

293 Which side of STS1 bus is reporting CTNEQPT alarm?

If Side A, replace CCM-A unit per DLP-101; then retrieve alarms.
If Side B, replace CCM-B unit per DLP-101; then retrieve alarms.

294 Did CTNEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

Table G. conddescr Parameters for CTNEQPT Alarm Generated by DMI, HIF, or LIF

CONDDESCR PARAMETERS	INTERNAL STS1 BUS SIDE IDENTIFIED BY PARAMETER
A1A2ERRORA_L1,_L2, or _L3 B2ERRORA_L1, _L2, or _ L3 ESALIGN_L1, _L2, or _L3 GBIAFAIL ISOCTNEQPT STS1AFAIL STS1AFAIL_L1, _L2, or _L3 STS1AFAILSW STS1AFAILSW_GBI STS1AFAILSW_L1, L2, or _L3 STS1AK2BAD STS1AK2BAD_GBI STS1AK2BAD_L1, _L2, or _L3 STSAINTERX_GBI STS1AINTERX STS1AINTERX_L1, _L2, or L3 DIAFAILSW_OC1, _OC2, _OC3, or _OC4	Side A

Table G. conddescr Parameters for CTNEQPT Alarm Generated by DMI, HIF, or LIF (cont)

CONDDESCR PARAMETERS	INTERNAL STS1 BUS SIDE IDENTIFIED BY PARAMETER
A1A2ERRORA_L1,_L2, or _L3	Side B
B2ERRORA_L1, _L2, or _ L3	
ESALIGN_L1, _L2, or _L3	
GBIBFAIL	
ISOCTNEQPT	
STS1BFAIL STS1BFAIL_L1, _L2, or _L3 STS1BFAILSW STS1BFAILSW_GBI STS1BFAILSW_L1, L2, or _L3	
STS1AK2BAB STS1BK2BAD_GBI STS1BK2BAB_L1, _L2, or _L3	
STSBINTERX_GBI STS1BINTERX STS1BINTERX_L1, _L2, or L3	
DIBFAILSW_OC1, _OC2, _OC3, _OC4	

295 STOP. This procedure is complete.

296 Replace the standby CCM unit per DLP-101; then retrieve alarms [DLP-100].

297 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 298.

298 Switch the active and standby CCM units and replace the CCM unit that is now in standby [DLP-505].

299 Retrieve alarms [DLP-100].

300 Did CTNEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

301 STOP. This procedure is complete.

Alarm/Condition – CTNEQPT (LDR)

302 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

303 Run diagnostics Phase 1 (NSA, LIF/LDR Control Bus test) on alarmed unit [DLP-500]. Perform 5 iterations.

304 Did diagnostics pass?

If yes, alarm may be intermittent. Go to step 305.
If no, then go to step 307.

305 Continue to monitor for CTNEQPT alarms. If alarm continues, go to step 307.

306 STOP. This procedure is complete.

307 Replace alarmed unit per DLP-101; then retrieve alarms [DLP-100].

308 Did CTNEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 309.

309 Retrieve alarms history log [DLP-528], and find record of CTNEQPT alarm.

310 Is the alarmed LDR an LDR501?

If yes, then go to step 313
If no, then continue to step 311.

311 In the work view, find the alarmed LDR in the Component column and CTNEQPT in the Conditions column. In the same row as the alarmed LDR and CTNEQPT, note the entry in the Details column.

NOTE: *BDITEST in the Details column indicates the failure came from the same-side LIF and XBDITEST indicates the failure came from the opposite-side LIF.*

312 Does BDITEST or XBDITEST appear in the Details column?

If BDITEST, replace same-side LIF [DLP-101]; then go to step 315.
If XBDITEST, replace opposite-side LIF [DLP-101]; then go to step 315.

313 In the view screen, find the alarmed LDR501 in the Component column and CTNEQPT in the Conditions column. In the same row as the alarmed LDR501 and CTNEQPT, note the entry in the Details column.

NOTE: *BDITEST_ACT in the Details column indicates the failure came from the active LIFD01 and BDITEST_STBY indicates the failure came from the standby LIFD01.*

314 Does BDITEST_ACT or BDITEST_STBY appear in the Details column?

If BDITEST_ACT, replace active LIFD01 [DLP-101]; then go to step 315.
If BDITEST_STBY, replace standby LIFD01 [DLP-101]; then go to step 315.

315 Retrieve alarms [DLP-100].

316 Did the CTNEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

317 STOP. This procedure is complete.

Alarm/Condition – FAILTOSW (CCM, DMI, or LIF)

318 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

319 Run diagnostic Phase 5 (NSA, Inter unit Communication Test) on alarmed unit [DLP-500]. Perform 5 iterations.

320 Did diagnostics pass?

If yes, alarm may be intermittent. Go to step 321.
If no, then go to step 323.

321 Continue to monitor for FAILTOSW alarms. If alarm continues, go to step 323.

322 STOP. This procedure is complete.

323 Replace the alarmed unit per DLP-101; then retrieve alarms [DLP-100].

324 Did FAILTOSW alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 325.

325 Were diagnostics run on opposite unit?

If yes, then continue to step 326.
If no, repeat from step 319 for opposite unit.

326 Are there any NEP or COA alarms?

If yes, return to step 3 and clear these alarms.
If no, contact Customer Service.

327 STOP. This procedure is complete.

Alarm/Condition – FAILTOSW (CLK)

328 Are there any other clock alarms?

If yes, return to step 3 and clear clock alarms.
If no, then continue to step 329.

329 Replace alarmed clock unit per DLP-101; then retrieve alarms [DLP-100].

330 Did FAILTOSW alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 331.

331 Replace other clock unit per DLP-101; then retrieve alarms [DLP-100].

332 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 333.

333 Are there any NEP alarms?

If yes, return to step 3 and clear NEP alarms.
If no, contact Customer Service.

334 STOP. This procedure is complete.

Alarm/Condition – FAILTOSW (LDR)

335 Replace standby LDR (or protection LDR if unit generating alarm is an LDR501) per DLP-101; then retrieve alarms [DLP-100].

336 Did FAILTOSW alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 337.

337 Replace the active LDR per DLP-101; then retrieve alarms [DLP-100].

338 Did FAILTOSW alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 339.

339 Replace the active LIF associated with LDR per DLP-101; then retrieve alarms [DLP-100].

340 Did FAILTOSW alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 341.

341 Replace standby LIF associated with LDR per DLP-101; then retrieve alarms [DLP-100].

342 Did FAILTOSW alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

343 STOP. This procedure is complete.

Alarm/Condition – FAILTOSW (VTG)

344 ***NOTE:*** *If the protection (P) VTG and another VTG are generating alarms, clear the protection VTG alarms first.*

Retrieve provisioned data for VTGs with lower numbers than alarmed VTG [DLP-502].

345 Are the preceding (lower number than the alarmed VTG) VTGs equipped and assigned?

If yes, then go to step 349.
If no, then continue to step 346.

346 **NOTE:** *Switching function relays on preceding VTGs need to be equipped.*

Equip the lower numbered VTGs.

347 Retrieve alarms [DLP-100].

348 Did FAILTOSW alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 349.

349 Retrieve provisioned data for VTG [DLP-502].

350 Is protection VTG(P) in active state (ACT)?

If yes, then continue to step 351.
If no (STBY), then go to step 352.

351 **NOTE:** *The protection VTG is already in use.*

Return to step 3 and clear other VTG alarms first.

352 Replace alarmed VTG unit per DLP-101; then retrieve alarms [DLP-100].

353 Did FAILTOSW alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 354.

354 Replace active DMI unit per DLP-101; then retrieve alarms [DLP-100].

355 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 356.

356 Replace adjacent VTG (to the left) per DLP-101; then retrieve alarms [DLP-100].

357 Did FAILTOSW alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 358.

358 Replace protection VTG per DLP-101; then retrieve alarms [DLP-100].

359 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 360.

360 Backplane relay control bus appears to be broken. Contact Customer Service.

361 STOP. This procedure is complete.

Alarm/Condition – FWCONTCOM or FWPROGFLT

362 **CAUTION: Possibility of service interruption. Reseating LIF901 unit interrupts ATM service.**

Reseat alarmed LIF901 unit; then retrieve alarms [DLP-100].

363 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 364.

364 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing the LIF901.**

Replace alarmed LIF901.

365 STOP. This procedure is complete.

Alarm/Condition – FWMJVER

366 Retrieve software inventory [DLP-537] and verify that Embedded Firmware Version and Inuse Firmware Version are different.

367 **CAUTION: Possibility of service interruption. The way to clear this alarm is to overwrite the Inuse Firmware on the Ethernet portion of the LIF901; however, overwriting the Inuse firmware interrupts service. Loss-of-service continues until the download is completed.**

To overwrite the Inuse firmware, either enable (allow) automatic download of firmware [DLP-532] or manually download firmware [DLP-533].

368 After downloading LAN firmware, retrieve alarms [DLP-100].

369 Did FWMJVER alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

370 STOP. This procedure is complete.

Alarm/Condition – FWMNVER

371 Retrieve software inventory [DLP-537].

372 On Software Inventory work view, note the minor version number of the Embedded Firmware and the Inuse Firmware.

373 Which version number is greater?

If Embedded Firmware, go to step 377 and overwrite Inuse firmware.
If Inuse Firmware, then continue to step 374.

374 **NOTE:** *The firmware loaded on the LIF901 is the most current version available, which is okay. If you want to silence the alarm, there are two ways to do it: perform a manual download to overwrite the Inuse firmware so the embedded firmware and Inuse firmware versions are the same or change the FWMNVER notification code to Not Reported.*

Do you want to silence the alarm?

If yes, then continue to step 375.
If no, STOP. This procedure is complete.

375 Do you want to silence alarm by changing the notification code or by overwriting the Inuse firmware?

If by notification code change, refer to DLP-534.
If firmware overwrite, then go to step 377.

376 STOP. This procedure is complete.

377 **CAUTION: Possibility of service interruption. Overwriting the Inuse firmware on the Ethernet portion of the LIF901 interrupts service. Loss-of-service continues until the download is completed.**

378 To overwrite the Inuse firmware, either enable (allow) automatic download of firmware [DLP-532] or manually download firmware [DLP-533].

379 STOP. This procedure is complete.

Alarm/Condition – HITEMP, LOTEMP or LPT

380 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

381 Replace HIF or LIF that is generating alarm; then retrieve alarms [DLP-100].

382 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, replace alarmed HIF or LIF at far end NE; then retrieve alarms.

383 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 384.

384 Perform transmission test on the fiber per local procedure.

385 STOP. This procedure is complete.

Alarm/Condition – IMPROPRMVL

386 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

387 Reinstall or replace unit that is generating alarm.

388 STOP. This procedure is complete.

Alarm/Condition – INHDGN

389 To clear alarm, allow diagnostics on the unit generating the alarm [DLP-522].

390 STOP. This procedure is complete.

Alarm/Condition – INHPMREPT

391 To clear alarm, allow PM reporting on the unit generating the alarm [DLP-510].

392 STOP. This procedure is complete.

Alarm/Condition – INHSWDX

393 **CAUTION: Possibility of service interruption. Under normal conditions, do not leave duplex switching inhibited.**

394 To clear alarm, allow duplex switching on the unit generating the alarm [DLP-506].

395 STOP. This procedure is complete.

Alarm/Condition – INHSWPR

396 **CAUTION: Possibility of service interruption. Under normal conditions, do not leave protection switching inhibited.**

397 To clear alarm, allow switching to protection unit [DLP-535].

398 STOP. This procedure is complete.

Alarm/Condition – INHSWWKG

399 To clear alarm, allow switching to working unit [DLP-536].

400 STOP. This procedure is complete.

Alarm/Condition – INT (CCM, COA, HIF, LDR, LIF, NEP, or VTG)

401 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

402 Replace alarmed unit per DLP-101; then retrieve alarms [DLP-100].

403 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 404.

404 Retrieve alarms [DLP-100] and check for other equipment alarms, especially alarms in a parent unit, NEP alarms, or PWR alarms.

405 Were other alarms found?

If yes, return to step 3 and clear those alarms.
If no, contact Customer Service.

406 STOP. This procedure is complete.

Alarm/Condition – INT (CLK)

407 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

408 Run diagnostic Phase 1 (NSA, Active NEP-CLOCK Communication test) on CLK unit [DLP-500]. Perform one iteration.

409 Did diagnostic phase pass?

If yes, NEP may be processing wrong message.
If no, then continue to step 410.

410 Replace alarmed clock unit per DLP-101; then retrieve alarms [DLP-100].

411 Did INT alarm clear?

If yes, STOP. This procedure is complete.
If no, suspect NEP is processing wrong message.

412 STOP. This procedure is complete.

Alarm/Condition – INT (DMI)

413 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

414 Retrieve alarms [DLP-100].

415 Is the alarm on the active DMI and is standby DMI available?

If yes, then continue to step 416.
If no, then go to step 417.

416 Switch DMIs [DLP-505].

417 Replace alarmed DMI per DLP-101; then retrieve alarms [DLP-100].

418 Did INT alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 419.

419 Are there any PWR alarms?

If yes, return to step 3 and clear PWR alarms.
If no, contact Customer Service.

420 STOP. This procedure is complete.

Alarm/Condition – INVERR (COA)

421 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

422 Replace COA unit per DLP-101; then retrieve alarms [DLP-100].

423 Did INVERR alarm clear?

If yes, STOP. This procedure is complete.
If no, check for NEP or other equipment alarms [DLP-100].

424 Were other alarms found?

If yes, return to step 3 and clear those alarms.
If no, contact Customer Service.

425 STOP. This procedure is complete.

Alarm/Condition – INVERR (LDR)

426 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

427 Replace alarmed LDR unit per DLP-101; then retrieve alarms [DLP-100].

428 Did INVERR alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 429.

429 ***NOTE:*** *Since LDR and LIF units in the same drop group share the bus on which the LDR reports its inventory, any one of the units on the bus may cause the alarm.*

What type of LDR is generating alarm?

If LDR501, then continue to step 430.
If LDR other than an LDR501, then go to step 433.

430 Replace an LDR501 unit per DLP-101; then retrieve alarms [DLP-100].

431 Did INVERR alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 432.

432 Have all LDR501 units been replaced?

If yes, go to step 435.
If no, return to step 430 and replace a different LDR501.

433 Replace the peer LDR unit per DLP-101; then retrieve alarms [DLP-100].

434 Did INVERR alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 435.

435 Replace standby LIF unit per DLP-101.

436 Did INVERR alarm clear?

If yes, STOP. This procedure is complete.
If no, replace active LIF unit per DLP-101.

437 STOP. This procedure is complete.

Alarm/Condition – INVERR (VTG)

438 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

439 Retrieve hardware inventory [DLP-537].

440 Was a response obtained?

If yes, go to step 442.
If no, replace VTG per DLP-101 because EEPROM is probably bad.

441 STOP. This procedure is complete.

442 Is data consistent with unit description?

If yes, error is intermittent; check for other VTG alarms.
If no, go to step 444.

443 STOP. This procedure is complete.

444 Check for NEP alarms [DLP-100].

445 Are there any NEP alarms?

If yes, then return to step 3 and clear NEP alarms.
If no, unit EEPROM is probably bad; go to step 446.

446 Are there any other VTG alarms?

If yes, go to step 3 and clear other VTG alarms.
If no, replace VTG per DLP-101.

447 STOP. This procedure is complete.

Alarm/Condition – INVERR (Generated by units other than COA, LDR, or VTG)

448 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

449 Retrieve hardware inventory [DLP-537].

450 Was a response obtained?

If yes, go to step 452.
If no, replace unit per DLP-101 because EEPROM is probably bad.

451 STOP. This procedure is complete.

452 Is data consistent with unit description?

If yes, error is intermittent. Check for other alarms [DLP-100].
If no, then go to step 453.

453 Retrieve alarms [DLP-100] and check for other alarms being generated by the alarmed unit, NEP alarms, or other equipment alarms.

454 Were other alarms found?

If yes, return to step 3 and clear those alarms.
If no, replace unit generating alarm because EEPROM is probably bad.

455 STOP. This procedure is complete.

Alarm/Condition – LBCL

456 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing an HIF or LIF to avoid interrupting service.**

Replace HIF or LIF generating alarm; then retrieve alarms [DLP-100].

457 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 458.

458 Are any PWR unit alarms being reported?

If yes, return to step 3 and clear PWR alarms.
If no, contact Customer Service.

459 STOP. This procedure is complete.

Alarm/Condition – MEA

460 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid interrupting service.**

461 Retrieve hardware inventory [DLP-537].

462 Was data retrieved successfully?

If yes, then continue to step 463.
If no, then go to step 469.

463 Retrieve provisioned parameters for the unit [DLP-502] and note provisioning of equipment type. Do not close work view.

464 From response, compare Equipment Type parameter to Unit Name.

465 Is database entry incorrect or is wrong unit installed?

If incorrect entry, then continue to step 466.
If wrong unit, then go to step 469.

466 Change provisioned value for Equipment Type [DLP-502].

NOTE: *Equipment type appears on plug_in unit faceplate.*

467 Retrieve alarms [DLP-100].

468 Did MEA alarm clear?

If yes, STOP. This procedure is complete.
If no, unit is not compatible with database entry; go to step 469.

469 Replace unit that is generating alarm [DLP-101].

470 STOP. This procedure is complete.

Alarm/Condition – MEMCHK

471 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

472 Copy database from NEP (working) to COA (primary) [DLP-538].

473 Did MEMCHK alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 474.

474 Replace COA per DLP-101; then retrieve alarms [DLP-100].

475 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

476 STOP. This procedure is complete.

Alarm/Condition – MEMDIF

477 **CAUTION: Possibility of service interruption. Copying the database incorrectly will interrupt service. If the COA was just replaced, clear other COA alarms first, if any exist. If the database is copied as described below, be certain to copy the database from working to primary to preserve system configuration (provisioning).**

478 Which unit has the preferred database?

If COA, copy primary database to working database [DLP-538]; then retrieve alarms [DLP-100].
If NEP, copy working database to primary database [DLP-538]; then retrieve alarms [DLP-100].

479 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 480.

480 Are there any other COA alarms?

If yes, return to step 3 and clear other COA alarms.
If no, contact Customer Service.

481 STOP. This procedure is complete.

Alarm/Condition – MEMDIFTRAN

482 **CAUTION: Possibility of service interruption. Except during an NE software upgrade, this alarm should be cleared by downloading the NEP with the same version of software the system (NE) is running.**

483 Is COA with expanded memory (program backup) available?

If yes, then continue to step 484.
If no, then go to step 486.

484 Copy database from COA (primary) to NEP (working) [DLP-538].

485 STOP. This procedure is complete.

486 Download version of software system is running to the NEP, either from a PC [DLP-566] or locally [DLP-568].

487 STOP. This procedure is complete.

Alarm/Condition – MEMVER

488 Was NEP or COA just replaced?

If NEP, then continue to step 489.
If COA, then go to step 494.

489 NEP has different version of software than system (COA database). Is COA with expanded memory (program backup) available?

If yes, then continue to step 490.
If no, then go to step 492.

490 Copy database from COA (primary) to NEP (working) [DLP-538].

491 STOP. This procedure is complete.

492 Download the version of software the system is running to the NEP, either from a PC [DLP-566] or locally [DLP-568].

493 STOP. This procedure is complete.

494 **CAUTION: Possibility of service interruption. The database on the COA has been overridden. Resolve other COA/NEP alarms, if any.**

495 Copy database from NEP (working) to COA (primary) [DLP-538].

496 STOP. This procedure is complete.

Alarm/Condition – MTCE

497 ***NOTE:*** *Since normal operations such as alarm generation and protection switching are inhibited when a unit is in maintenance state, it should not be left in this state for an extended period of time.*

To clear this alarm, place unit in-service [DLP-501].

498 STOP. This procedure is complete.

Alarm/Condition – PLLEOR

499 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a clock to avoid interrupting service.**

500 To clear this alarm, replace the clock that is generating the alarm.

501 STOP. This procedure is complete.

Alarm/Condition – PROGFLT

502 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

503 Replace unit generating alarm because EEPROM is probably bad.

504 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

505 STOP. This procedure is complete.

Alarm/Condition – PROGVER

506 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

507 Retrieve software inventory and compare software versions on the NEP and the alarmed unit [DLP-521].

508 Are program versions the same on NEP and the alarmed unit?

If yes, then go to step 509.
If no, then go to step 511.

509 Replace alarmed unit per DLP-101; then retrieve alarms [DLP-100].

510 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 514.

511 Download software to the inconsistent unit, either from a PC [DLP-566] or locally [DLP-568]; then retrieve alarms [DLP-100].

512 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 513.

513 Was alarmed unit replaced?

If yes, then go to step 514.
If no, then go to step 509.

514 Contact Customer Service.

515 STOP. This procedure is complete.

Alarm/Condition – PROTNA (LDR501 or VTG)

516 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

517 ***NOTE:*** *If a protection unit is not available, all working LDR501s or VTGs generate a PROTNA alarm.*

Do you want a protection LDR or VTG?

If yes, then go to step 519.
If no, unassign protection LDR or VTG unit [DLP-501].

518 STOP. This procedure is complete.

519 Check equipment status of LDR or VTG to the left of the unit with a PROTNA alarm.

520 Replace the LDR or VTG to the left of the unit with the PROTNA alarm per DLP-101; then retrieve alarms [DLP-100].

521 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

522 STOP. This procedure is complete.

Alarm/Condition – PROTNA (LIFF01)

523 OC3 assignment between A and B side must match. To clear this alarm, assign an OC3 on the opposite side of the drop group if one side is already assigned.

NOTE: *An LIFF01 generates this alarm only if the NE is equipped with a CCM101.*

524 STOP. This procedure is complete.

Alarm/Condition – SWEQPT

525 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid interrupting service.**

526 Run diagnostic Phase 1 (Active VTG Relay Control Bus test) and Phase 2 (Inactive VTG Relay Control Bus test) on alarmed VTG [DLP-500]. Perform 5 iterations.

527 Did diagnostics pass?

If yes, then continue to step 528.
If no, then go to step 535.

528 Retrieve alarms [DLP-100].

529 Are there any DMI alarms?

If yes, return to step 3 and clear DMI alarms.
If no, then continue to step 530.

530 Replace the standby DMI per DLP-101; then retrieve alarms [DLP-100].

531 Did SWEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 532.

532 Replace the active DMI per DLP-101; then retrieve alarms [DLP-100].

533 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

534 STOP. This procedure is complete.

535 Replace the alarmed VTG per DLP-101; then retrieve alarms [DLP-100].

536 Did SWEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 537.

537 Are there any DMI alarms?

If yes, return to step 3 and clear DMI alarms.
If no, then continue to step 538.

538 In step 526, which unit failed diagnostics: active, standby or both?

If both, then continue to step 539.
If active or standby, then go to step 541.

539 ***NOTE:*** *If both failed and the VTG has been replaced, there may be a backplane problem.*

Contact Customer Service.

540 STOP. This procedure is complete.

541 Based on the diagnostic results, replace the active or standby DMI per DLP-101; then retrieve alarms [DLP-100].

542 Did SWEQPT alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

543 STOP. This procedure is complete.

Alarm/Condition – SYNC (CCM)

544 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid interrupting service.**

545 Retrieve CCM alarms [DLP-100].

546 Is there a SYNCCLK alarm?

If yes, then go to step 595.
If no, then continue to step 547.

547 Replace alarmed CCM per DLP-101; then retrieve alarms [DLP-100].

548 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 549.

549 Replace the opposite side CLK (i.e., if alarmed CCM is on Side A, replace CLKB, and if alarmed CCM is on Side B, replace CLKA). Refer to DLP-101.

550 Retrieve alarms [DLP-100].

551 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 552.

552 Replace the same side CLK unit per DLP-101; then retrieve alarms [DLP-100].

553 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

554 STOP. This procedure is complete.

Alarm/Condition – SYNC (HIF or LIF)

555 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid interrupting service.**

556 Retrieve alarms [DLP-100].

557 Is there a SYNCCLK alarm?

If yes, then go to step 595.
If no, then continue to step 558.

558 Replace alarmed unit per DLP-101; then retrieve alarms [DLP-100].

559 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 560.

560 Replace the CCM unit on the opposite side of the alarmed unit (i.e., if alarmed unit is on Side A, replace CCM-B, and if alarmed unit is on Side B, replace CCM-A). Refer to DLP-101.

561 Retrieve alarms [DLP-100].

562 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 563.

563 Replace the same side CCM unit per DLP-101; then retrieve alarms [DLP-100].

564 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

565 STOP. This procedure is complete.

Alarm/Condition – SYNC (NEP)

566 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid interrupting service.**

567 Retrieve alarms [DLP-100].

568 Is there an SYNCCLK alarm?

If yes, then go to step 595.
If no, then continue to step 569.

569 ***NOTE:*** *The autonomous message, REPT ALM EQPT with an aid of NEP, most likely includes a conddescr parameter. The conddescr parameter is either CLK**A**FAIL or CLK**B**FAIL. The highlighted A or B in the conddescr parameter indicates which CCM clock input failed.*

Do you have a record of an autonomous message associated with the SYNC alarm?

If yes, then go to step 571.
If no, then continue to step 570.

570 Retrieve alarm history [DLP-528] and find record of SYNC alarm.

571 Does the autonomous record include a conddescr parameter?

If yes, then continue to step 572.
If no, then go to step 577.

572 Was the conddescr parameter CLKAFAIL or CLKBFAIL?

If CLKAFAIL, replace CCM-A per DLP-101; then retrieve alarms.
If CLKBFAIL, replace CCM-B per DLP-101; then retrieve alarms.

573 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 574.

574 Replace the NEP per DLP-101; then retrieve alarms [DLP-100].

575 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

576 STOP. This procedure is complete.

577 Replace the NEP per DLP-101; then retrieve alarms [DLP-100].

578 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 579.

579 Replace CCM-A unit per DLP-101; then retrieve alarms [DLP-100].

580 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 581.

581 Replace CCM-B unit per DLP-101; then retrieve alarms [DLP-100].

582 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

583 STOP. This procedure is complete.

Alarm/Condition – SYNC (VTG)

584 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid interrupting service.**

585 ***NOTE:*** *The VTG cannot sync with the incoming (demux) signal or the outgoing (mux) signal.*

Retrieve alarms [DLP-100].

586 In the same digroup, are there any other VTG units generating alarms?

If yes, then go to step 589.
If no, then continue to step 587.

587 Replace the alarmed VTG per DLP-101; then retrieve alarms [DLP-100].

588 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 589.

589 Are there any DMI alarms?

If yes, return to step 3 and clear DMI alarms.
If no, then continue to step 590.

590 Replace the standby DMI per DLP-101; then retrieve alarms [DLP-100].

591 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 592.

592 Replace the active DMI per DLP-101; then retrieve alarms [DLP-100].

593 Did SYNC alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

594 STOP. This procedure is complete.

Alarm/Condition – SYNCCLK (CCM)

595 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

596 Are there any clock alarms?

If yes, return to step 3 and clear CCM alarms.
If no, then continue to step 597.

597 Replace alarmed CCM per DLP-101; then retrieve alarms [DLP-100].

598 Did SYNCCLK alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 599.

599 Retrieve CCM alarms [DLP-100].

600 From the response, determine whether the alarmed CCM is receiving clock input from CLK-A unit (CLKSELA) or CLK-B (CLKSELB).

601 Replace CLK unit that is providing clock to alarmed CCM per DLP-101; then retrieve alarms [DLP-100].

602 Did SYNCCLK alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 603.

603 Suspect backplane problem. Contact Customer Service.

604 STOP. This procedure is complete.

Alarm/Condition – SYNCCLK (CLK)

605 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

606 Retrieve CLK conditions [DLP-100] and determine if alarmed unit is active or standby.

607 Is alarmed unit in standby?

If yes, then continue to step 608.
If no, then go to step 610.

608 Replace the alarmed unit per DLP-101; then retrieve alarms [DLP-100].

609 Did SYNCCLK alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 614.

610 Was there an INHSWDX alarm?

If yes, then go to step 393.
If no, then continue to step 611.

611 Does standby unit have a more severe alarm or is it absent?

If more severe alarm, return to step 3 and clear that alarm first.
If standby unit is absent, then continue to step 612.

612 Install missing CLK unit per DLP-101; then retrieve alarms [DLP-100].

613 Did SYNCCLK alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 614.

614 Is there an alarm on the other CLK unit?

If yes, return to step 3 and clear alarm on other CLK unit.
If no, then continue to step 615.

615 Check for NEP alarms or source alarms (OC3, OC12, OC48, or BITS). Go to TAP-001.

616 STOP. This procedure is complete.

Alarm/Condition – SYNCCLK (DMI, HIF, or LIF)

617 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

618 ***NOTE:*** *CCM or CLK alarms and equipment alarms reported as ISLTD (isolated) should be cleared first.*

Are there any other equipment alarms?

If yes, return to step 3 and clear other alarms.
If no, then continue to step 619.

619 Replace alarmed unit per DLP-101; then retrieve alarms [DLP-100].

620 Did SYNCCLK alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 621.

621 Replace the CCM unit on the same side as the alarmed unit (i.e., if alarmed unit is on Side A, replace CCM-A, and if alarmed unit is on Side B, replace CCM-B). Refer to DLP-101.

622 Retrieve alarms [DLP-100].

623 Did alarms clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 624.

624 Replace other side CCM unit per DLP-101; then retrieve alarms [DLP-100].

625 Did SYNCCLK alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 626.

626 Suspect backplane problem. Contact Customer Service.

627 STOP. This procedure is complete.

Alarm/Condition – SYNCCLK (NEP)

628 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

629 Were there any CCM alarm conditions (INT, SYNCCLK, IMPROPRML, or MEA)?

If yes, return to step 3 and clear CCM alarms.
If no, then continue to step 630.

630 Replace NEP per DLP-101; then retrieve alarms [DLP-100].

631 Did SYNCCLK alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 632.

632 Replace CCM-A per DLP-101; then retrieve alarms [DLP-100].

633 Did SYNCCLK alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 634.

634 Replace CCM-B per DLP-101; then retrieve alarms [DLP-100].

635 Did SYNCCLK alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

636 STOP. This procedure is complete.

Alarm/Condition – SYNCCLK (VTG)

637 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

638 Retrieve alarms [DLP-100].

639 Is there more than one VTG with a SYNCCLK alarm?

If yes, then go to step 642.
If no, then continue to step 640.

640 Replace the alarmed VTG per DLP-101; then retrieve alarms [DLP-100].

641 Did SYNCCLK alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 642.

642 Replace the active DMI unit per DLP-101; then retrieve alarms [DLP-100].

643 Did SYNCCLK alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 644.

644 Replace the standby DMI unit per DLP-101; then retrieve alarms [DLP-100].

645 Did SYNCCLK alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

646 STOP. This procedure is complete.

Alarm/Condition – SYNCSEL

647 **CAUTION: Possibility of service interruption. Adhere to DLP-101 in the following steps when replacing a plug-in unit to avoid interrupting service.**

Replace the standby (STBY) LIF per DLP-101; then retrieve alarms [DLP-100].

648 Did SYNCSEL alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 649.

649 Replace active (ACT) LIF per DLP-101; then retrieve alarms [DLP-100].

650 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 651.

651 Sequentially replace LIFs in other drops groups and retrieve alarms after each replacement [DLP-100].

652 Did SYNCSEL alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

653 STOP. This procedure is complete.

Alarm/Condition – TRMT

654 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid interrupting service.**

Replace the alarmed LDR per DLP-101; then retrieve alarms [DLP-100].

655 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 656.

656 What type of LDR is generating the alarm?

If LDR101, 201, or 301, then go to step 657.
If LDR501, then go to step 664.

657 ***NOTE:*** *TRMT alarm could be a result of the parent LIF not receiving the LDR TX alarm interrupt.*

Run diagnostic Phase 2 (NSA, LDR Transmit Alarm) on alarmed LDR. Perform 5 iterations. [DLP-500].

658 On the Diagnostics work view, select the i (Information) icon.

659 From the Information Details window, determine whether the active or standby LIF did not receive the LDR TX alarm interrupt.

If active LIF did not receive interrupt, then go to step 660.
If standby LIF did not receive interrupt, then go to step 662.

660 Replace active LIF per DLP-101; then retrieve alarms [DLP-100].

661 Did TRMT alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 664

662 Replace standby LIF per DLP-101; then retrieve alarms [DLP-100].

663 Did TRMT alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 664.

664 Contact Customer Service.

665 STOP. This procedure is complete.

TAP-022
Clear EC1 Alarm

Purpose

Provides procedures for clearing EC1 alarms.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Retrieve alarms [DLP-100].
2	Are there any LIF or LDR alarm indications on drop group with alarmed EC1? If yes, go to TAP-021 and clear alarm(s). If no, go to step 3.
3	Is far-end terminal a 1603 SMX, 1603 SM, or 1603 SE Network Element (NE)? If yes, go to step 5. If no, go to step 4.
4	Go to far-end terminal and resolve alarms per vendor's documentation. If no problems are found, go to step 7.
5	Retrieve alarms at the far-end 1603 SMX, 1603 SM, or 1603 SE NE [DLP-100].
6	Are there any LIF or LDR alarm indications at the far end? If yes, go to TAP-021 and clear alarm(s). If no, go to step 7.
7	Have EC1 alarms and conditions been retrieved? If yes, go to step 9. If no, go to step 8.

8 Retrieve EC1 alarms and conditions [DLP-100].

9 Locate the alarm or condition in Table A; then go to the step indicated to clear it.

Table A. Alarms/Conditions/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
AISL	Line alarm indication signal. Either a failure has occurred at the far-end terminal or the EC1 facility is removed from service due to loopback or other tests.	10
APSB	Automatic Protection Switch Byte failure. The K1/K2 byte is invalid.	20
BERL-HT	Bit Error Ratio Line — High (NEND RCV). The number of bits in error to the number of bits transmitted has degraded to the point of exceeding a set threshold.	22
BERL-LT	Bit Error Ratio Line — Low (NEND RCV)	22
INHPMREPT	Inhibit all scheduled PM reports. Autonomous reporting of performance monitoring data has been inhibited on the EC1 facility.	108
LOF	Loss of frame (NEND RCV). An out-of-frame condition has lasted for more than 3 ms.	110
LOS	Loss of signal (NEND RCV). The receive signal has been lost, an all zeros pattern has lasted for more than 100 ms, or clock recovery has been lost.	110
MTCE	EC1 facility has been removed from service for maintenance	118
RFI	Remote Failure Indication. An upstream defect has occurred along the line in the mux direction.	105
SECTRCMF	Section Trace Mismatch. The expected section tracer and the incoming section tracer are different. Either the section tracer is incorrectly provisioned at one end of the SONET section or the intended traffic is not being received.	120
SYNCLEVINFAIL	Synchronization level input failure	134
T-BPV	Bipolar violations TCA*	150
T-CVL	Coding violations — Line TCA* (NEND RCV)	150
	Coding violations — Line TCA* (FEND RCV)	150
T-CVS	Coding violations — Section TCA*	150
T-ESL	Errored seconds — Line TCA* (NEND RCV)	150
	Errored seconds — Line TCA* (FEND RCV)	150
T-ESS	Errored seconds — Section TCA*	150
T-SEFS	Severely errored framing seconds TCA*	150

Table A. Alarms/Conditions/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
T-SESL	Severely errored seconds – Line TCA* (NEND RCV)	150
	Severely errored seconds – Line TCA* (FEND RCV)	150
T-SESS	Severely errored seconds – Section TCA*	150
T-UASL	Unavailable seconds – Line TCA* (NEND RCV)	150
	Unavailable seconds – Line TCA* (FEND RCV)	150
Condition	**Description**	**Action**
ACTLPBK	Loopback active	No action
AINS	Automatic-In-Service state	No action
SYNCLEVIN-( )	Input synchronization message value (0...15)	No action
SYNCLEVOUT-( )	Output synchronization message value (0...15)	No action
Event	**Description**	**Action**
ACTLPBK	Loopback active	No action
AINS	Automatic In-Service state	No action
IS-AUTO	Automatic OOS-MA to IS	No action
SECTRCHG	Section trace change	No action
SYNCLEVINCHG	Synchronization level input change	No action
* *TCA = Threshold Crossing Alert*		

Alarm/Condition – AISL

10 Is far-end terminal a 1603 SMX, 1603 SM, or 1603 SE Network Element (NE)?

If yes, go to step 13.
If no, go to step 11.

11 Go to far-end terminal and resolve alarms per vendor's documentation.

12 STOP. This procedure is complete.

13 From office records, determine which drop group (DG1, DG2, DG3, or DG4) provides the EC1 facility interface at the far-end NE.

14 Log on to the far-end NE [DLP-117] and retrieve EC1 alarms [DLP-100].

15 Is ACTLPBK (active loopback) reported?

If yes, go to step 16.
If no, go to step 18.

16 Determine if tests are in progress. If no tests are in progress, release loopback [DLP-523].

17 STOP. This procedure is complete.

18 Retrieve alarms [DLP-100] and resolve any equipment or facility alarms that are reported (refer to TAP-001).

19 STOP. This procedure is complete.

Alarm/Condition – APSB

20 Are there any other EC1 alarms?

If yes, return to step 9.
If no, go to step 29 and follow LIF/LDR testing procedure for BERL-HT/BERL-LT alarms.

21 STOP. This procedure is complete.

Alarm/Condition – BERL-HT and BERL-LT

22 Check coax cable connections at 1603 SMX backplane and cross-connection panel. Correct connections, if necessary.

23 If connections are correct, retrieve Line Buildout parameter at far-end NE (perform the following if NE is a 1603 SMX, 1603 SM, or 1603 SE) [DLP-525].

24 Compare the provisioning of Line Buildout parameter to office records (refer to Table B for recommended setting based on cable types).

Table B. Line Buildout Settings

TYPE AND DISTANCE OF CABLE	DISTANCE (FEET)	SETTING*
AT&T 728A or equivalent cable	0–225	Yes
AT&T 728A or equivalent cable	226–450	No
AT&T 734A or equivalent cable	0–200	Yes
AT&T 734A or equivalent cable	201–400	No
AT&T 735A or equivalent cable	0–110	Yes
AT&T 735A or equivalent cable	111–220	No

* *The Line Buildout setting (Yes or No) depends on the type of coax cable used and the distance to the STS1 cross-connect.*

25 Does Line Buildout parameter need to be changed?

If yes, go to step 26.
If no, go to step 29.

26 Change provisioning of Line Buildout parameter at the far-end NE [DLP-525].

27 Retrieve alarms [DLP-100].

28 Did alarm clear (may take several minutes to clear)?

If yes, STOP. This procedure is complete.
If no, go to step 29.

29 **CAUTION: Possibility of service interruption. When replacing an LIF or LDR, adhere to the procedure in DLP-101 to avoid service interruption.**

30 Locate the type of LIF associated with the EC1 facility reporting the alarm in Table C; then go to the step indicated to clear the alarm.

Table C. Types of LIFs

IF DROP GROUP IS EQUIPPED WITH AN...	AND UNIT IS...	THEN GO TO...
LIF201	Non-redundant	Step 31
	Redundant	Step 47
LIF501/701	Non-redundant	Step 31
	Redundant	Step 69
LIFD01	Non-redundant	Step 78
	Redundant	Step 92

Non-redundant LIF201 or LIF501/701 Unit

31 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF and LDR units. If EC1 facility is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

32 Place LIF to be diagnosed in maintenance state [DLP-501].

33 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

34 Did diagnostics pass?

If yes, go to step 37.
If no, go to step 35.

35 Replace LIF per DLP-101.

36 STOP. This procedure is complete.

37 Place LIF back in-service [DLP-501].

38 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR.**

39 Place LDR to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

40 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

41 Did diagnostics pass?

If yes, go to step 44.
If no, go to step 42.

42 Replace LDR per DLP-101.

43 STOP. This procedure is complete.

44 Place LDR back in-service [DLP-501].

45 Problem must be at far-end terminal. Analyze alarms per TAP-001 at far-end NE. If problem persists, test coax facility per local procedure or contact Customer Service.

46 STOP. This procedure is complete.

Redundant LIF201 Unit

NOTE: *The active and standby LIFs will be switched to determine whether the active LIF or active LDR is causing the alarm.*

47 Switch to redundant LIF [DLP-505].

NOTE: *When LIF20x units are switched, the LDRs also switch (i.e., LDR-A is active when LIF-A is active, and LDR-B is active when LIF-B is active).*

48 Retrieve alarms [DLP-100].

49 Did alarm clear (may take several minutes)?

If yes, go to step 52.
If no, go to step 50.

50 Problem must be at far-end terminal. Analyze alarms per TAP-001 at far-end NE. If problem persists, test coax facility per local procedure or contact Customer Service.

51 STOP. This procedure is complete.

52 Problem must be in standby LIF or LDR. Go to step 53 and perform diagnostics on LIF.

53 **CAUTION: Possibility of service interruption. Some diagnostic phases are service-affecting if performed on an active unit. Be sure the LIF and LDR units are in maintenance state before performing diagnostics.**

54 Place LIF to be diagnosed in maintenance state (OOS-MT-MAN) [DLP-501].

55 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

56 Did diagnostics pass?

If yes, go to step 59.
If no, go to step 57.

57 Replace LIF per DLP-101.

58 STOP. This procedure is complete.

59 Place LIF back in-service [DLP-501].

60 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR. Perform the following on standby side if LIF and LDR are redundant.**

61 Place LDR to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

62 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

63 Did diagnostics pass?

If yes, go to step 66.
If no, go to step 64.

64 Replace LDR per DLP-101.

65 STOP. This procedure is complete.

66 Place LDR back in-service [DLP-501].

67 Analyze alarms per TAP-001 at far-end NE. If problem persists, test coax facility per local procedure or contact Customer Service.

68 STOP. This procedure is complete.

Redundant LIF501/701 Unit

NOTE: *The active and standby LIFs associated with the alarmed facility will be switched to determine whether the active LIF is causing the alarm. If the alarm isn't cleared, the active and standby LDRs associated with the alarmed facility will be switched.*

69 Switch to redundant LIF [DLP-505]; then retrieve alarms [DLP-100].

70 Did alarm clear (may take several minutes)?

If yes, replace standby LIF per DLP-101.
If no, go to step 72.

71 STOP. This procedure is complete.

72 Switch to LDR [DLP-505]; then retrieve alarms [DLP-100].

73 Did alarm clear (may take several minutes)?

If yes, go to step 74.
If no, go to step 76.

74 Replace standby LDR per DLP-101.

75 STOP. This procedure is complete.

76 Problem must be at far-end terminal. Analyze alarms per TAP-001 at far-end NE. If problem persists, test coax facility per local procedure or contact Customer Service.

77 STOP. This procedure is complete.

Non-redundant LIFD01 Unit

NOTE: *Diagnostics will be performed on the LIF associated with the alarmed facility. If diagnostics pass, the protection LDR and the LDR associated with the alarmed facility will be switched.*

78 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF unit. If EC1 facility is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

79 Place LIF to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

80 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

81 Did diagnostics pass?

If yes, go to step 83.
If no, replace LIF per DLP-101.

82 STOP. This procedure is complete.

83 Place LIF back in-service [DLP-501].

84 Switch the LDR501 that is carrying the alarmed EC1 facility to protection [DLP-529]. (For help in identifying the LDR refer to DLP-565.)

85 Retrieve alarms [DLP-100].

86 Did alarm clear (may take several minutes)?

If yes, go to step 87.
If no, go to step 89.

87 Replace the LDR501 that was switched to protection [DLP-101]. (For help in identifying the physical location of the LDR, refer to DLP-565.)

88 STOP. This procedure is complete.

89 If switch back to working was inhibited, allow automatic switching to working unit [DLP-536].

90 Problem must be at far-end terminal. Analyze alarms per TAP-001 at far-end NE.

If problem persists, test coax facility per local procedure or contact Customer Service.

91 STOP. This procedure is complete.

Redundant LIFD01 Unit

NOTE: *The active and standby LIFs associated with the alarmed facility will be switched to determine whether the active LIF is causing the alarm. If the alarm isn't cleared, the protection LDR and the LDR associated with the alarmed facility will be switched.*

92 Switch to redundant LIF [DLP-505].

93 Retrieve alarms [DLP-100].

94 Did alarm clear (may take several minutes)?

If yes, go to step 95.
If no, go to step 97.

95 Replace standby LIF per DLP-101.

96 STOP. This procedure is complete.

97 Switch the LDR501 that is carrying the alarmed EC1 facility to protection [DLP-529]. (For help in identifying the LDR refer to DLP-565.)

NOTE: *Revertive switch may occur. Inhibit switch back to working if required.*

98 Retrieve alarms [DLP-100].

99 Did alarm clear (may take several minutes)?

If yes, go to step 100.
If no, go to step 102.

100 Replace the LDR501 that was switched to protection [DLP-101]. (For help in identifying the physical location of the LDR, refer to DLP-565.)

101 STOP. This procedure is complete.

102 If switch back to working was inhibited, allow automatic switching to working unit [DLP-536].

103 Problem must be at far-end terminal. Analyze alarms per TAP-001 at far-end NE. If problem persists, test coax facility per local procedure or contact Customer Service.

104 STOP. This procedure is complete.

Alarm/Condition – RFI

105 **NOTE:** *The far-end equipment generates the RFI (line) signal when it detects LOS, LOF or Line AIS. APS signaling is used to convey failure information from one NE/equipment to another. Because the far-end equipment could be manufactured by another vendor, this procedure cannot specify alarms to identify at the other end.*

Retrieve alarms at the far end NE [DLP-100].

106 Go to TAP-001 to find the appropriate TAP to resolve the alarm.

107 STOP. This procedure is complete.

Alarm/Condition – INHPMREPT

108 To clear alarm, allow PM reporting on EC1 facility [DLP-510].

109 STOP. This procedure is complete.

Alarm/Condition – LOF and LOS

110 Check coax cable connections at 1603 SMX backplane and cross-connection panel. Correct connections, if necessary.

111 If connections are okay, retrieve Line Buildout parameter at far-end NE [DLP-525].

112 Compare the provisioning of Line Buildout to office records (refer to Table B for recommended setting based on cable types).

113 Does Line Buildout parameter need to be changed?

If yes, go to step 114.
If no, go to step 116.

114 Change Line Buildout parameter at the far-end NE [DLP-525]; then retrieve alarms [DLP-100].

115 Did alarm clear (may take several minutes to clear)?

If yes, STOP. This procedure is complete.
If no, go to step 116.

116 Go to step 30 and follow LIF/LDR testing procedure at near-end NE (i.e., NE with alarm).

117 STOP. This procedure is complete.

Alarm/Condition – MTCE

118 To clear alarm, restore EC1 facility to in-service [DLP-501].

119 STOP. This procedure is complete.

Alarm/Condition – SECTRCMF

120 Do you want section trace enabled?

If yes, go to step 123.
If no, go to step 121.

121 Disable monitoring of the section trace [DLP-546].

122 STOP. This procedure is complete.

123 Retrieve section trace data [DLP-547] and compare the Expected Incoming value with the Received Incoming value.

124 From office records, determine which value is wrong.

If Expected Incoming, go to step 125.
If Received Incoming, go to step 127.

125 Change expected incoming value to match the received incoming section tracer [DLP-547].

126 STOP. This procedure is complete.

127 Log on at the far-end NE that is supposed to terminate this EC1 facility [DLP-117].

128 At the far end NE, retrieve provisioned expected section trace information [DLP-547].

129 Does Trace Format = TR1 (Provisionable Format) and does Provisioned Outgoing value = the value expected at the near end [0...255]?

If yes, go to step 130.
If no, go to step 132.

130 An incorrect cross-connection in the facility is the most probable cause. Troubleshoot facility per local procedures.

131 STOP. This procedure is complete.

132 Change the far end Provisioned Outgoing value to match the Expected Incoming value at the near end [DLP-547].

133 STOP. This procedure is complete.

Alarm/Condition – SYNCLEVINFAIL

134 Retrieve current synchronization conditions [DLP-100].

135 Note the number following **SYNCLEVIN**.

NOTE: *The number following SYNCLEVIN is the synchronization status message (expressed as a decimal number). This message is contained in the S1 portion (bits 5-6-7-8) of the S1/Z1 byte in the STS frame transport overhead.*

136 Is the synchronization status message a valid value (0, 1, 4, 7, 10, 12, 13, 14, or 15)?

If yes, go to step 137.
If no, go to step 143.

137 In the first column of Table D, find the value obtained in step 135.

NOTE: *The other columns define the quality level and the synchronization traceability that correspond to that synchronization status message.*

Table D. Interpretation of SYNCLEVIN Message Values

SYNCHRONIZATION STATUS MESSAGE	QUALITY LEVEL		SYNCHRONIZATION TRACEABILITY
	1ST GENERATION (V1)	2ND GENERATION (V2)	
0	2	2	Traceability Unknown
1	1	1	Stratum 1 Traceable
4	N/A	4	Transit Node Clock Traceable
7	3	3	Stratum 2 Traceable
10	4	6	Stratum 3 Traceable
12	5	7	Minimum Clock Traceable
13	N/A	5	Stratum 3E Traceable
14	User assignable	User assignable	Reserved for network sync
15	7	9	Don’t use for synchronization

138 Is the quality level 1, 2, 3, or 4?

If no, then go to step 139.
If yes, go to step 141.

139 Network synchronization provisioning is probably not correct. Contact Customer Service.

140 STOP. This procedure is complete.

141 Retrieve synchronization conditions [DLP-100].

142 Is the synchronization message value the same as it was when you checked it the first time?

If yes, contact Customer Service.
If no, the synchronization value is changing; go to step 143.

143 Retrieve alarms [DLP-100].

144 Are there other EC1 facility alarms?

If yes, return to step 9 and clear other EC1 alarms.
If no, go to step 145.

145 Are there any equipment alarms?

If yes, go to TAP-021.
If no, go to step 146.

146 Have alarms been retrieved at the adjacent NE?

If yes, go to step 148.
If no, go to step 147.

147 Perform steps 143 through 145 at the adjacent NE (i.e., the NE that is transmitting data for the alarmed facility).

148 Contact Customer Service.

149 STOP. This procedure is complete.

Alarm/Condition – T-xxx

NOTE: *A threshold crossover alert (TCA) has been generated because one of the performance parameters exceeds the value specified for it (refer to Table E).*

Table E. EC1 PM Thresholds

MONITOR TYPE	FACTORY DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERL-HT	4		3...4	Bit Error Ratio Line – High threshold (SFBER)
BERL-LT	7		5...9	Bit Error Ratio Line – Low threshold (DGBER)
BPV	443	4428	1...4,294,967,295	Bipolar violations
CVL	443	4428	1...4,294,967,295	Coding violation line count (near end or far end)
CVS	448	4470	1...4,294,967,295	Coding violation count – Section
DSESL	2500		1...65535	Number of coding violations to make one SESL
DSESS	2500		1...65535	Number of coding violations to make one SESS
ESL	12	100	1...65535	Line Errored Seconds (near end or far end)
ESS	12	100	1...65535	Section Errored Seconds
SEFS	2	17	1...65535	Severely Errored Framing Seconds – OOFS/COFAS
SESL	3	7	1...65535	Line Severely Errored Seconds (near end or far end)
SESS	3	7	1...65535	Section Severely Errored Seconds
UASL	10	10	1...65535	Line Unavailable Seconds (near end or far end)

150 Retrieve current conditions for EC1 facility [DLP-100].

151 Are there any other EC1 facility alarms (besides T-xxx)?

If yes, go to step 152.
If no, go to step 154.

152 Return to step 9 and clear other EC1 facility alarms first.

153 STOP. This procedure is complete.

154 Is the condition severe enough to warrant unit replacement?

If yes, go to step 156.
If no, record the alarm as an event.

155 STOP. This procedure is complete.

156 From the work view opened in step 150, determine location of T-xxx condition.

157 Is location of T-xxx condition Near End or Far End?

If Near End, go to step 158.
If Far End, go to step 161.

158 ***NOTE:*** *The near end is detecting a problem on the receive (facility) side. Problem is most likely at far-end equipment or on facility.*

Troubleshoot equipment and facility alarms at far-end terminal.

159 If problem is not found, suspect facility. Troubleshoot and repair facility per local practices.

160 STOP. This procedure is complete.

161 ***NOTE:*** *The far end is detecting a problem on the receive (facility) side. Problem is most likely at near-end equipment or on the facility.*

162 **CAUTION: Possibility of service interruption. When replacing an LIF or LDR, adhere to the procedure in DLP-101 to avoid service interruption.**

163 Refer to Table F and locate the type of LIF associated with the EC1 facility reporting the alarm. Go to the step referenced in the table to clear the alarm.

Table F. Types of LIFs

IF DROP GROUP IS EQUIPPED WITH AN...	AND UNIT IS...	THEN GO TO...
LIF201	Non-redundant	Step 164
	Redundant	Step 180
LIF501/701	Non-redundant	Step 164
	Redundant	Step 202
LIFD01	Non-redundant	Step 213
	Redundant	Step 227

Non-redundant LIF201 or LIF501/701 Unit

164 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF and LDR units. If EC1 facility is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

165 At the near-end NE, place LIF to be diagnosed in maintenance state (OOS-MT-MAN) [DLP-501].

166 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

167 Did diagnostics pass?

If yes, go to step 170.
If no, go to step 168.

168 Replace LIF per DLP-101.

169 STOP. This procedure is complete.

170 Place LIF back in-service [DLP-501].

171 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR.**

172 Place LDR to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

173 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

174 Did diagnostics pass?

If yes, go to step 177.
If no, go to step 175.

175 Replace LDR per DLP-101.

176 STOP. This procedure is complete.

177 Place LDR back in-service [DLP-501].

178 Problem most likely in facility. Troubleshoot per local practice.

179 STOP. This procedure is complete.

Redundant LIF201 Unit

NOTE: *The active and standby LIFs will be switched to determine whether the active LIF or active LDR is causing the alarm.*

180 Switch to redundant LIF [DLP-505].

NOTE: *When LIF20x units are switched, the LDRs also switch, (i.e., LDR-A is active when LIF-A is active, and LDR-B is active when LIF-B is active).*

181 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves register values.*

182 Did PM errors stop?

If yes, go step 185.
If no, go to step 183.

183 Problem most likely in facility. Troubleshoot per local practice.

184 STOP. This procedure is complete.

185 Problem must be in standby LIF or LDR. Go to step 186 and perform diagnostics on LIF.

186 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LIF. Be sure the LIF is in maintenance state before performing diagnostics.**

187 Place LIF to be diagnosed in maintenance state (OOS-MT-MAN) [DLP-501].

188 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

189 Did diagnostics pass?

If yes, go to step 192.
If no, go to step 190.

190 Replace LIF per DLP-101.

191 STOP. This procedure is complete.

192 Place LIF back in-service [DLP-501].

193 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR. Be sure the LDR unit is in maintenance state before performing diagnostics.**

194 Place LDR to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

195 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

196 Did diagnostics pass?

If yes, go to step 199.
If no, go to step 197.

197 Replace LDR per DLP-101.

198 STOP. This procedure is complete.

199 Place LDR back in-service [DLP-501].

200 Problem most likely in facility. Troubleshoot per local practice.

201 STOP. This procedure is complete.

Redundant LIF501/701 Unit

NOTE: *The active and standby LIFs associated with the alarmed facility will be switched to determine whether the active LIF is causing the alarm. If the alarm isn't cleared, the active and standby LDRs associated with the alarmed facility will be switched.*

202 Switch to redundant LIF [DLP-505]; then retrieve alarms [DLP-100].

203 Did alarm clear (may take several minutes)?

If yes, go to step 204.
If no, go to step 206.

204 Replace standby LIF per DLP-101.

205 STOP. This procedure is complete.

206 Switch to redundant LDR [DLP-505].

207 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves register values.*

208 Did PM errors stop?

If yes, go step 209.
If no, go to step 211.

209 Replace standby LDR per DLP-101.

210 STOP. This procedure is complete.

211 Problem most likely in facility. Troubleshoot per local practice.

212 STOP. This procedure is complete.

Non-redundant LIFD01 Unit

NOTE: *Diagnostics will be performed on the LIF associated with the alarmed facility. If diagnostics pass, the protection LDR and the LDR associated with the alarmed facility will be switched.*

213 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF unit. If EC1 facility is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

214 Place LIF to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

215 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

216 Did diagnostics pass?

If yes, go to step 218.
If no, replace LIF per DLP-101.

217 STOP. This procedure is complete.

218 Place LIF back in-service [DLP-501].

219 Switch the LDR501 that is carrying the alarmed EC1 facility to protection [DLP-529]. (For help in identifying the AID of the LDR refer to DLP-565.)

220 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves register values.*

221 Did PM errors stop?

If yes, go step 222.
If no, go to step 224.

222 Replace the LDR501 that was switched to protection [DLP-101]. (For help in identifying the physical location of the LDR, refer to DLP-565.)

223 STOP. This procedure is complete.

224 If switch back to working was inhibited, allow automatic switching to working unit [DLP-536].

225 Problem most likely in facility. Troubleshoot per local practice.

226 STOP. This procedure is complete.

Redundant LIFD01 Unit

NOTE: *The active and standby LIFs associated with the alarmed facility will be switched to determine whether the active LIF is causing the alarm. If the alarm isn't cleared, the protection LDR and the LDR associated with the alarmed facility will be switched.*

227 Switch to redundant LIF [DLP-505].

228 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves register values.*

229 Did PM errors stop?

If yes, go step 230.
If no, go to step 232.

230 Replace standby LIF per DLP-101.

231 STOP. This procedure is complete.

232 Switch the LDR501 that is carrying the alarmed EC1 facility to protection [DLP-529]. (For help in identifying the AID of the LDR, refer to DLP-565.)

NOTE: *Revertive switch may occur. Inhibit switch back to working if required.*

233 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves register values.*

234 Did PM errors stop?

If yes, go step 235.
If no, go to step 237.

235 Replace the LDR501 that was switched to protection [DLP-101]. (For help in identifying the physical location of the LDR, refer to DLP-565.)

236 STOP. This procedure is complete.

237 If switch back to working was inhibited, allow automatic switching to working unit [DLP-536].

238 Problem most likely in facility. Troubleshoot per local practice.

239 STOP. This procedure is complete.

TAP-023
Clear X.25 Alarm or X.25 Failure

Purpose

Provides procedures for clearing X.25 alarm or X.25 failure.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

There are several possible causes for X.25 communications not working:

- Physical connection broken between the Gateway Network Element and the Packet Switched Network (PSN)
- Far-end X.25 node is not ready
- Wrong COA is installed. An odd-numbered COA (i.e., COA601, 603, 605, etc.) must be installed.
- Port has been deleted
- *X*.25 stack is provisioned out-of-service.

STEP	PROCEDURE
1	Was a LAPBERR alarm received? ***NOTE:*** *LAPBERR is a Link Access Protocol Balanced (LAPB) error, which is synonymous with a physical layer error of the X.25 interface.* If yes, go to step 2. If no, go to step 14.
2	Check the X.25 interface wire-wrap connections on the rear of the shelf; repair if necessary.
3	Was there a problem? If yes, go to step 4. If no, go to step 6.

4 Retrieve alarms [DLP-100].

5 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 6.

6 Make contact at the far end and verify that the X.25 interface equipment is turned ON and ready, and the X.25 cable is connected. Correct, if required.

7 Was there a problem on the far end?

If yes, go to step 8.
If no, go to step 10.

8 Retrieve alarms at far end [DLP-100].

9 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 10.

10 Per local practices, perform a continuity check of the wiring between the Gateway Network Element and the far-end X.25 equipment. Correct, if required.

11 Was there a problem?

If yes, correct problem; then go to step 12.
If no, contact Customer Service.

12 Retrieve alarms [DLP-100].

13 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

14 ***NOTE:*** *No LAPBERR alarm was received and X.25 communications is not working.*

Verify that the 1603 SMX shelf is equipped with an odd numbered COA (i.e., COA601, 603, 605, etc.) and the COA is not in an alarm state.

15 Was odd numbered COA installed?

If yes, go to step 16.
If no, install odd numbered COA.

16 Retrieve provisioned data for X.25 ports [DLP-502].

17 On X.25 Provision Parameters work view, note the Primary State of X.25 port. Is it in-service (IS) or out-of-service (OOS)?

If IS, go to step 18.
If OOS, go to step 20.

18 Retrieve provisioned data for X.25 protocols [DLP-502].

19 On X.25 Protocol work view, note the Service State of X.25 Protocol. Is it in-service (IS) or out-of-service (OOS)?

If IS, go to step 27.
If OOS-MA-UAS, go to step 24.

20 Place X.25 port in-service [DLP-501].

21 Change service state of X.25 protocol to in-service [DLP-501].

22 Contact the Operations System and determine if the X.25 interface is working.

23 Is the problem resolved?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

24 The X.25 stack has not been provisioned for in-service. Change service state of X.25 protocol to in-service [DLP-501].

25 Contact the Operations System and determine if the X.25 interface is working.

26 Is the problem resolved?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

27 ***NOTE:*** *Since the X.25 port function is installed and provisioned in-service, and the X.25 stack is in-service, and no X.25 port alarm is present, the only remaining possibility is corrupted virtual circuits (one or both).*

Remove the X.25 port from service (Unassign); then place it back in-service [DLP-501].

28 Contact the Operations System to determine if the X.25 interface is working.

29 Is the problem resolved?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

30 STOP. This procedure is complete.

TAP-024
Clear Fan Faults

Purpose

Provides procedures for clearing fan faults.

Prerequisites

Nonflammable heat source and a Digital Volt Meter (DVM) are required.

General

Fans are optionally equipped as needed per site requirements.

STEP	PROCEDURE
1	See Figure 1 to determine fan assembly location(s).
2	Refer to the fuse assignment chart on the Power Distribution Unit (PDU) or the Fuse and Alarm Panel (FAP) to identify fan fuse.
3	Verify that fan fuse is good; replace fuse if blown.
4	On the fan assemblies, set the NORMAL/DISABLE switch(es) to the NORMAL position.
5	Allow a few seconds for fans to start and stabilize.
6	Are any fan alarm LEDs (1–4) lighted on the fan assemblies? If yes, go to step 11 and replace fan assembly. If no, go to step 7.
7	Is ambient temperature greater than 100°F (37.8°C)? If yes, go to step 8. If no, go to step 9.
8	Are all fans running? If yes, go to step 9. If no, go to step 11 and replace fan assembly that is not running.

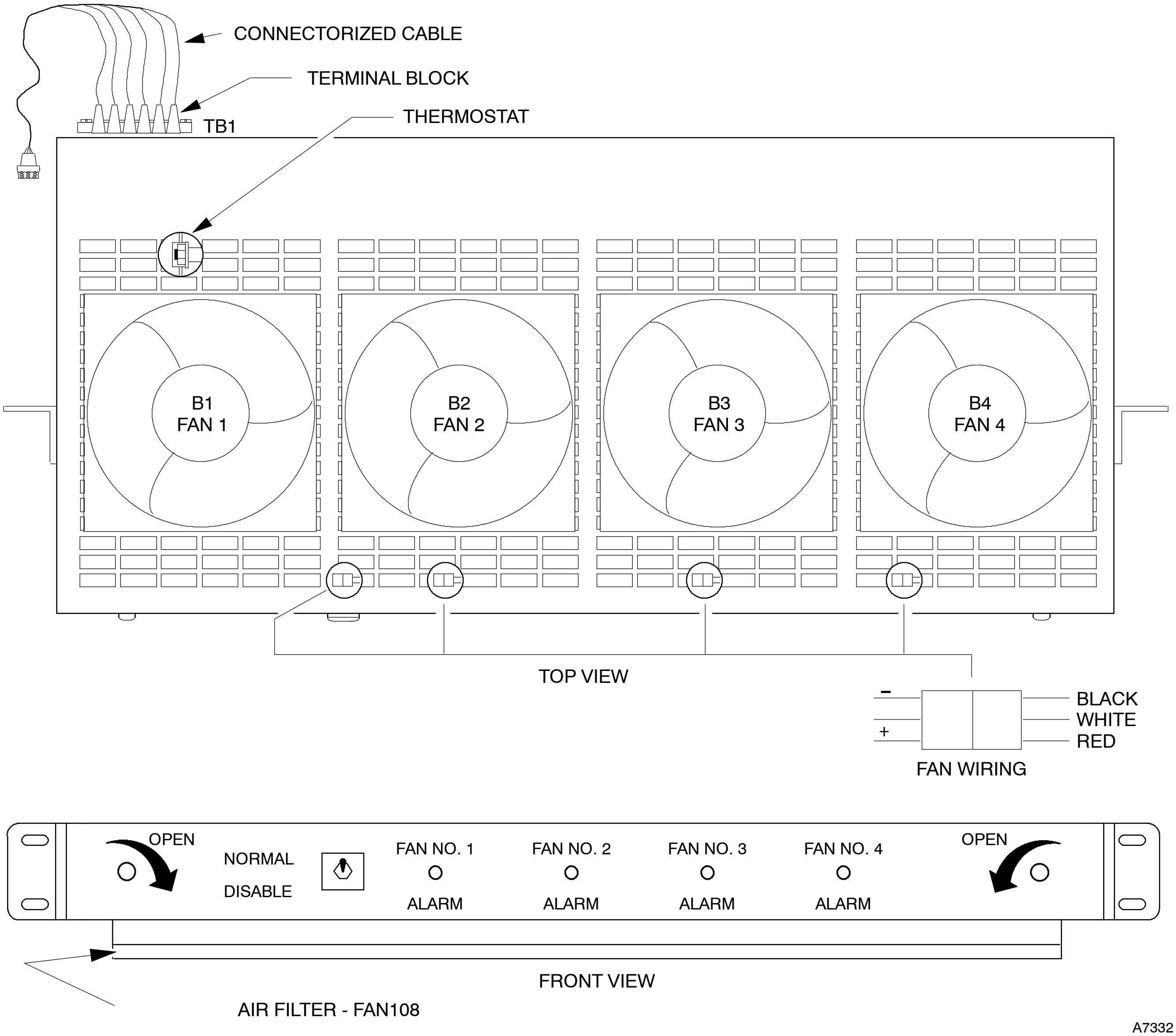


Figure 1. Fan Assembly Typical Layout

9 ***NOTE:*** *Fans are thermostatically controlled to turn on and off. If two fan assemblies are equipped, power is supplied to both assemblies through the thermostat in the top assembly. The fans can be forced on by applying heat to the top thermostat.*

Apply and remove heat. Verify that fans turn on and off as temperature rises and falls (Table A).

Table A. Fan On and Off Temperatures

MNEMONIC	GROUP	ON	OFF
FAN102	-002	38°C	29°C
FAN104	-004	38°C	29°C

10 Do fans turn on and off as temperature rises and falls?

If yes, go to step 16.
If no, go to step 11.

11 Unlatch fan assembly and slide the assembly out.

12 Set the NORMAL/DISABLE switch to the DISABLE position.

13 Replace the faulty fan with a spare unit (600976-713-001).

14 Set the NORMAL/DISABLE switch to the NORMAL position and verify fan operation per step 9.

15 Slide fan assembly back into the shelf and secure the latches.

16 STOP. This procedure is complete.

TAP-025
Clear Fuse and Alarm Panel (FAP) Alarm

Purpose

Provides procedures for clearing a FAP alarm.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific Network Elements (NEs).

STEP	PROCEDURE
1	Identify the alarm (see Figure 1). If Fuse, go to step 2. If Critical, Major, or Minor, go to step 8.

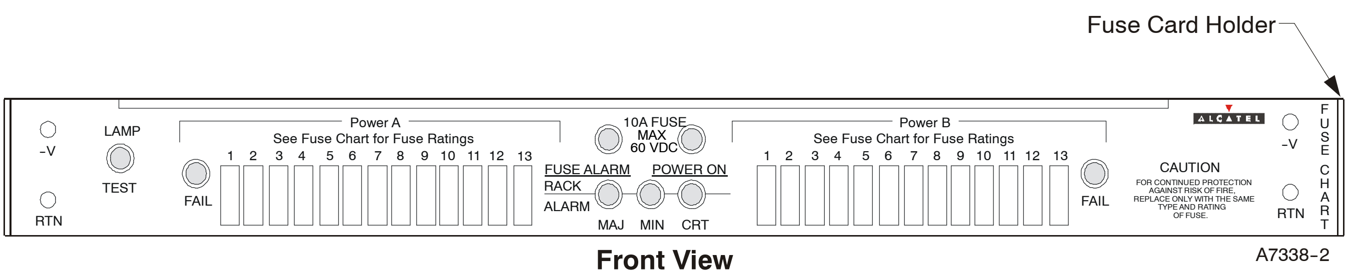


Figure 1. Fuse and Alarm Panel

STEP	PROCEDURE
2	Look for blown fuse on the fuse distribution panel (see Figure 1).
3	Remove blown fuse and identify amperage or color.
4	Place good fuse in holder.
5	Did the new fuse blow? If yes, go to step 6. If no, STOP. This procedure is complete.

6 Check configuration chart for what the fuse supplies and resolve that problem; check for shorts with a DVM or equivalent.

7 STOP. This procedure is complete.

8 Examine the network elements being served by the fuse panel (see configuration chart attached to front of fuse panel, Figure 1).

9 Inspect the COA unit on each NE for a critical alarm.

10 Retrieve all active alarms [DLP-100].

11 From the response, identify unit and clear alarm. Refer to TAP-001.

12 STOP. This procedure is complete.

TAP-027
Clear NE Sync (SYNCN) Alarm

Purpose

Provides procedures for clearing NE Sync alarms.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) through the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Retrieve alarms [DLP-100].
2	Are there any equipment or facility alarms? If yes, go to step 3. If no, go to step 4.
3	Resolve equipment and facility alarms first per TAP-001.
4	Locate the alarm or condition in Table A; then go to the referenced step to clear it.

Table A. NESYNC Alarms/Condition/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
( )-DG1A-n*	Drop Group 1, Side A – Facility 1...4 sync reference has failed.	5
( )-DG1B-n*	Drop Group 1, Side B – Facility 1...4 sync reference has failed.	5
( )-DG2A-n*	Drop Group 2, Side A – Facility 1...4 sync reference has failed.	5
( )-DG2B-n*	Drop Group 2, Side B – Facility 1...4 sync reference has failed.	5

Table A. NESYNC Alarms/Condition/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
( )-DG3A-n*	Drop Group 3, Side A — Facility 1…4 sync reference has failed.	5
( )-DG3B-n*	Drop Group 3, Side B — Facility 1…4 sync reference has failed.	5
( )-DG4A-n*	Drop Group 4, Side A — Facility 1…4 sync reference has failed.	5
( )-DG4B-n*	Drop Group 4, Side B — Facility 1…4 sync reference has failed.	5
( )-LG1A*	Line Group 1, Side A sync reference has failed	11
( )-LG1B*	Line Group 1, Side B sync reference has failed	11
( )-LG2A*	Line Group 2, Side A sync reference has failed	11
( )-LG2B*	Line Group 2, Side B sync reference has failed	11
( )-SYNCPRI*	Sync primary BITS input reference has failed	16
( )-SYNCSEC*	Sync secondary BITS input reference has failed	25
FRNG	Free Running. Clock entered free-running mode for one of the following reasons: NE sync reference list is not provisioned; a power-up occurred and 200 seconds have not elapsed; or the Prov Sync Mode parameter is provisioned as Free Running.	34
FST	Fast. Clock entered fast mode because either the Prov Sync Mode parameter is provisioned as Fast Sync or phase relationship fell out of Normal mode.	51
HLDOVR	Synchronization is in holdover mode	79
INHAUTOMODESW	Automatic switching to primary timing reference is inhibited	98
INHPMREPT	Scheduled PM reports are inhibited	100
LOCKOUTOFSYNC	Lockout of Synchronization. The sync source has toggled in and out too often (i.e., more than five times in fifteen minutes) to establish a good sync source.	107
OPRACT	Operate Active. A manual switch to a synchronization reference is in effect.	112
SYNC	High speed synchronization references have failed	102
SYNCSWFAIL	Synchronization reference switch failure. Clock (CLK) is unable to select appropriate synchronization reference source.	118

Table A. NESYNC Alarms/Condition/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
Condition	**Description**	**Action**
DELAYSWSYNC	Synchronization switch mode delayed (provisioned)	No action
FRNGSYNC	Free running synchronization mode (provisioned)	No action
FSTSYNC	Fast start synchronization mode (provisioned)	No action
HLDOVRSYNC	Hold-over synchronization mode (provisioned)	No action
IMEDSWSYNC	Synchronization switch mode is immediate (provisioned)	No action
OPRSYNC-PRI	Operate synchronization on primary reference	No action
OPRSYNC-SEC	Operate synchronization on second reference	No action
OPRSYNC-THIRD	Operate synchronization on third reference	No action
OPRSYNC-FOURTH	Operate synchronization on fourth reference	No action
OPRSYNC-FIFTH	Operate synchronization on fifth reference	No action
Event	**Description**	**Action**
MANSWTOPRI	Manual switch to primary reference	No action
MANSWTOSEC	Manual switch to secondary reference	No action
MANSWTOTHIRD	Manual switch to 3rd priority reference	No action
MANSWTOFOURTH	Manual switch to 4th priority reference	No action
MANSWTOFIFTH	Manual switch to 5th priority reference	No action
SWTOPRI	Automatic switch to primary reference	No action
SWTOSEC	Automatic switch to secondary reference	No action
SWTOTHIRD	Automatic switch to 3rd priority reference	No action

Table A. NESYNC Alarms/Condition/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
SWTOFOURTH	Automatic switch to 4th priority reference	No action
SWTOFIFTH	Automatic switch to 5th priority reference	No action
SWTOINT	Automatic switch to internal clock reference	No action
* *The condition/alarm may have prefix (PRI-, SEC-, THIRD, FOURTH or FIFTH).*		

Alarm/Condition – ( )-DGxx

5 Retrieve alarms [DLP-100].

6 Are there any LIF alarms?

If yes, go to TAP-021.
If no, go to step 7.

7 Are there any OC3 or OC12 facility alarms?

If yes, go to TAP-029.
If no, go to step 8.

8 Are there EC1 facility alarms?

If yes, go to TAP-022.
If no, go to step 9.

9 Are there any clock (CLK) or NEP alarms?

If yes, go to TAP-021.
If no, contact Customer Service.

10 STOP. This procedure is complete.

Alarm/Condition – ( )-LGxx

11 Retrieve alarms [DLP-100].

12 Are there any HIF alarms?

If yes, go to TAP-021.
If no, go to step 13.

13 Are there any line group OC facility alarms?

If yes, go to TAP-029.
If no, go to step 14.

14 Are there any clock (CLK) or NEP alarms?

If yes, go to TAP-021.
If no, contact Customer Service.

15 STOP. This procedure is complete.

Alarm/Condition – ( )-SYNCPRI

16 Retrieve alarms [DLP-100].

17 Are there any BITS facilities alarms?

If yes, go to TAP-012.
If no, go to step 18.

18 Are there any CLK alarms?

If yes, go to TAP-021.
If no, go to step 19.

19 **CAUTION: Possibility of service interruption. Adhere to procedures in DLP-101 when replacing the CLK unit to avoid interrupting service.**

20 Replace CLK-A per DLP-101; then retrieve alarms [DLP-100].

21 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 22.

22 Replace CLK-B per DLP-101; then retrieve alarms [DLP-100].

23 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

24 STOP. This procedure is complete.

Alarm/Condition – ( )-SYNCSEC

25 Retrieve alarms [DLP-100].

26 Are there any BITS facilities alarms?

If yes, go to TAP-012.
If no, go to step 27.

27 Are there any CLK alarms?

If yes, go to TAP-021.
If no, go to step 28.

28 **CAUTION: Possibility of service interruption. Adhere to procedures in DLP-101 when replacing the CLK unit to avoid interrupting service.**

29 Replace CLK-B per DLP-101; then retrieve alarms [DLP-100].

30 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 31.

31 Replace CLK-A per DLP-101; then retrieve alarms [DLP-100].

32 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

33 STOP. This procedure is complete.

Alarm/Condition – FRNG

34 Retrieve provisioned NE sync parameters and note the first Selected Reference in the Sync Reference Order region on the work view [DLP-502].

35 Is the first Selected Reference INT (internal clock)?

If yes, go to step 36.
If no, go to step 38.

36 ***NOTE:*** *A FRNG condition is normal if the NE is not provisioned for network synchronization (i.e., primary reference [first selected reference] is INT). If NE is in a network and is (or will be) carrying traffic, the NE must be provisioned for network synchronization. Refer to the 1603 SMX Provisioning Guide.*

Provision NE for synchronization before placing it in-service.

37 STOP. This procedure is complete.

38 Was the NE just powered up?

If yes, go to step 39.
If no, go to step 41.

39 Wait four minutes; then retrieve alarms [DLP-100].

40 Did FRNG alarm clear?

If yes, STOP. This procedure is complete.
If no, return to step 34.

41 Is Prov Sync Mode parameter provisioned Free Running?

If yes, go to step 42.
If no, go to step 45.

42 ***NOTE:*** *For normal operation, free running mode is not recommended.*

Do you want to change synchronization mode to normal?

If yes, go to step 43.
If no, STOP. This procedure is complete.

43 On NE Sync Provision Parameters work view, change Prov Sync Mode parameter to normal [DLP-502].

44 STOP. This procedure is complete.

45 Retrieve alarms [DLP-100].

46 Are there any other alarms?

If yes, go to step 47.
If no, go to step 49.

47 Resolve equipment, facilities, and SYNCN alarms per TAP-001.

48 STOP. This procedure is complete.

49 Contact Customer Service.

50 STOP. This procedure is complete.

Alarm/Condition – FST

51 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid interrupting service.**

52 Retrieve provisioned NE Sync parameters and in Current Status region on work view, note Sync Mode [DLP-502].

53 Is Sync Mode Fast Sync?

If yes, go to step 54.
If no, go to step 57.

54 **NOTE:** *For normal operation, Fast Sync is not recommended.*

Do you want to change mode to normal?

If yes, go to step 55.
If no, STOP. This procedure is complete.

55 Change Prov Sync Mode parameter to Normal [DLP-502].

56 STOP. This procedure is complete.

57 **NOTE:** *Phase lock loop is wandering. Problems in network (if NE is loop-timed) or BITS source may cause CLK units to go into FST mode. Otherwise, a CLK unit may be faulty.*

Are both CLK-A and CLK-B units equipped?

If yes, go to step 59.
If no, go to step 58.

58 **NOTE:** *Problem may be in network.*

Wait at least one hour and if alarm persists, replace active CLK unit per DLP-101; then go to step 71.

59 Do both NESYNCA and NESYNCB have an FST alarm?

If yes, go to step 63.
If no, go to step 60.

60 Is it NESYNCA or NESYNCB that has the FST alarm?

If NESYNCA, replace CLKA per DLP101; then go to step 61.
If NESYNCB, replace CLKB per DLP101; then, go to step 61.

61 Wait 15 minutes; then retrieve alarms [DLP-100].

62 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

63 Problem is probably in network. Retrieve provisioned NE sync parameters [DLP-502].

64 On the NE Sync Provision Parameters work view, note the alternate sync sources. Is an alternate sync source available besides the one that is currently active?

If yes, go to step 65.
If no, go to step 70.

65 Switch to another sync source and release [DLP-503].

66 Wait 15 minutes; then retrieve alarms [DLP-100].

67 Did FST alarm clear?

If yes, go to step 68.
If no, go to step 70.

68 Problem exists on facility that was switched from. Resolve problems per TAP-001.

69 STOP. This procedure is complete.

70 Wait at least one hour; then retrieve alarms [DLP-100]. If alarm persists, replace active CLK unit per DLP-101.

71 Wait 15 minutes; then retrieve alarms [DLP-100].

72 Did FST alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 73.

73 Is CLK redundant?

If yes, go to step 74.
If no, go to step 77.

74 Replace other CLK unit per DLP-101.

75 Wait 15 minutes; then retrieve alarms [DLP-100].

76 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then go to step 77.

77 Contact Customer Service.

78 STOP. This procedure is complete.

Alarm/Condition – HLDOVR

Holdover mode may occur under the following conditions:

- Under command
- During the time period between selection of a new reference and stabilization
- During the time period between sync problem and declaring it unavailable
- When phase relationship falls out of fast mode
- When sync reference is unavailable and there is no other reference.

79 Was phase relationship set to fast mode (FST)?

If yes, circuit may not be stable enough to keep it in FST window causing it to go into Holdover mode. Go to step 51.
If no, go to step 80.

80 Retrieve provisioned NE Sync parameters and note Prov Sync Mode in the Current Status region on the work view [DLP-502].

81 Is Prov Sync Mode parameter Holdover for NESYNC (A/B)?

If yes, go to step 82.
If no, go to step 85.

82 ***NOTE:*** *For normal operation, a provisioned Holdover condition is not recommended.*

Do you want to change synchronization mode to normal?

If yes, go to step 83.
If no, STOP. This procedure is complete.

83 Change Prov Sync Mode parameter on NE Sync Provision Parameters work view to Normal [DLP-502].

84 STOP. This procedure is complete.

85 Was the Sync Reference Order recently changed?

If yes, go to step 86.
If no, go to step 90.

86 Wait five minutes; then retrieve NESYNC conditions [DLP-100].

87 Is HLDOVR alarm still active?

If yes, go to step 88.
If no, STOP. This procedure is complete.

88 Reevaluate sync sources.

NOTE: *Synchronization mode may have changed from Normal to Fast and from Fast to Holdover.*

89 Retrieve alarms [DLP-100].

90 Are there any source reference alarms on sync referenced facilities or equipment?

If yes, go to step 91.
If no, go to step 92.

91 Clear these alarms first. Go to TAP-001.

92 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing the CLK unit to avoid interrupting service.**

93 Replace standby CLK unit per DLP-101; then retrieve alarms [DLP-100].

94 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 95.

95 Replace other CLK unit per DLP-101; then retrieve alarms [DLP-100].

96 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

97 STOP. This procedure is complete.

Alarm/Condition – INHAUTOMODESW

98 To clear alarm, allow automatic synchronization restoration switching [DLP-558].

99 STOP. This procedure is complete.

Alarm/Condition – INHPMREPT

100 To clear alarm, allow PM reporting [DLP-510].

101 STOP. This procedure is complete.

Alarm/Condition – SYNC

102 Is NE initially being powered up?

If yes, go to step 103.
If no, go to step 105.

103 Wait five minutes for stabilization.

104 STOP. This procedure is complete.

105 A reference sync source has failed; resolve clock or other NE sync alarm. Return to step 1.

106 STOP. This procedure is complete.

Alarm/Condition – LOCKOUTOFSYNC

107 ***NOTE:*** *The NE automatically clears a LOCKOUTOFSYNC state if it continues for four hours.*

Do you want to switch to a preferred source?

If yes, go to step 108.
If no, STOP. This procedure is complete.

108 Switch to an alternate sync source and release [DLP-503].

109 Retrieve alarms [DLP-100].

110 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

111 STOP. This procedure is complete.

Alarm/Condition – OPRACT

112 **CAUTION: Possibility of service interruption. While the OPRACT alarm is active, normal synchronization switching is inhibited. Do not leave OPRACT alarm active during normal operation.**

113 Is there a valid need to keep manual reference switch in effect?

If yes, STOP. This procedure is complete.
If no, go to step 114.

114 Release sync switch [DLP-503].

115 Retrieve alarms [DLP-100].

116 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

117 STOP. This procedure is complete.

Alarm/Condition – SYNCSWFAIL

118 Retrieve alarms [DLP-100].

119 Are there any equipment alarms?

If yes, go to step 120.
If no, go to step 122.

120 ***NOTE:*** *All unit alarms are indicated on the COA unit by severity level (CR [Critical], MJ [Major], or MN [Minor]). If there is a COA CONTCOM and an NEP alarm, resolve the COA alarm first.*

Identify the alarmed unit with the highest severity; then go to TAP-021 to clear the alarm.

121 STOP. This procedure is complete.

122 Are there any facility alarms?

If yes, go to TAP-001.
If no, go to step 123.

123 Switch to primary sync source and release [DLP-503].

124 Retrieve alarms [DLP-100].

125 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 126.

126 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing the CLK unit to avoid interrupting service.**

127 Replace the CLK that is active per DLP-101; then retrieve alarms [DLP-100].

128 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

129 STOP. This procedure is complete.

TAP-029
Clear OCn (OC3, OC12, or OC48) Facility Alarm

Purpose

Provides procedures for clearing OC3, OC12, and OC48 alarms for line groups and drop groups equipped with SONET optical facilities

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Have alarms and conditions been retrieved? If yes, then go to step 3. If no, then continue to step 2.
2	Retrieve OC alarms and conditions [DLP-100].
3	Locate the alarm you want to clear in Table A; then go to step indicated to clear it.

Table A. OCn Facility Alarms/Conditions/Events

IF ALARM/ CONDITION IS...	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
AISL	OC3, OC12, or OC48	4	Alarm Indication Signal—Line. A line alarm indication signal has been detected from upstream.
ALS	OC3, OC12, or OC48	11	Automatic Laser Shutdown. The transmit laser automatically shut off when Loss-of-Signal (LOS) was detected on the optical receiver.
APSB	OC3, OC12, or OC48	26	Automatic Protection Switch Byte failure. A request to switch did not occur or a K1 byte value was invalid or inconsistent. Most likely cause is a problem with the NE at the other end of the OC span.
APSCM	OC3, OC12, or OC48	50	Automatic Protection Switch Channel Match failure. Received K2 byte did not match transmitted K1 byte.

Table A. OCn Facility Alarms/Conditions/Events (cont)

IF ALARM/ CONDITION IS...	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
APSDFLT	OC48 facility in receive direction	74	Receive Automatic Protection Switch Default. The node at the other end of a span is not able to perform BLSR ring switching operations because it has no knowledge of ring map and node ID.
APSDFLT	OC48 facility in transmit direction	89	Transmit Automatic Protection Switch Default. NE is not able to perform BLSR ring switching because of BLSR configuration errors. This alarm occurs briefly after an NE is powered up.
APSIMPROP	OC48	99	Improper Automatic Protection Switch Code (BLSR). Three consecutive and identical frames have occurred that contain the following irregularities: unused codes in bits 6-8 of K2; codes irrelevant to the specific protection switching operation request; and requests irrelevant to the state of the ring.
APSINCON	OC48	106	Twelve consecutive frames occurred and no 3 consecutive frames contained identical APS bytes.
APSMM	OC3, OC12, or OC48	50	Automatic Protection Switch Mode Mismatch. The connecting NE at the far end is in a different APS mode than the near-end NE.
APSNODEIDMM	OC48	111	Automatic Protection Switch Node ID Mismatch failure (BLSR). Three consecutive and identical frames were received that contain a source node that does not match a neighbor's Node ID or an entry in the ring map.
BERL-HT	OC3, OC12, or OC48	114	Bit Error Ratio Line — High Threshold crossed. The ratio of the number of bits in error to the number of bits received has degraded to the point of exceeding a set threshold.
BERL-LT	OC3, OC12, or OC48	114	Bit Error Ratio Line — Low Threshold crossed. The bit error ratio exceeds a threshold setting between 10^{-5} and 10^{-9}.
FAILTOSW	OC3, OC12, or OC48	123	Failure to Switch. The OC facility failed to switch to protection equipment.
FAILTOSW-RING	OC48	132	Failure to Switch — Ring. BLSR ring failed to switch.
FEPRLF	OC3, OC12, or OC48	137	Far-End Protection Line Failure. The autoprotection at the far end has failed.

Table A. OCn Facility Alarms/Conditions/Events (cont)

IF ALARM/ CONDITION IS...	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
FRCD	OC3, OC12, or OC48	144	Forced. An operate protection switch command was executed on a facility that has the switch mode set to FRCD (forced).
FRCD-RING	OC48	141	A forced BLSR ring switch request is in effect.
INHEX-RING	OC48	147	Inhibit Exercise Tests (BLSR). The automatic ring switch exercise has been inhibited.
INHPMREPT	OC3, OC12, or OC48	149	Inhibit PM Reports. Autonomous reporting of performance monitoring data has been inhibited on an OC facility.
LINENA	OC3, OC12, or OC48	151	Line Not Available. Line is not available because of a detected failure in the mux direction.
LOCKOUTOFPR	OC3, OC12, or OC48	144	Lockout of Protection. An operate protection switch command was executed on a facility with the switch mode set to Lockout.
LOCKOUT-LOWR	OC48	158	A BLSR ring lockout switch request is in effect for the local NE.
LOCKOUT-LPS	OC48	161	A BLSR ring lockout switch request is in effect for the entire ring.
LOF	OC3, OC12, or OC48	164	Loss of Frame. An out-of-frame condition has persisted for more than 3 msec.
LOS	OC3, OC12, or OC48	164	Loss of Signal. Probable causes: loss of a receiver signal; an all zeros pattern for over 100 ms; or clock recovery is lost. A poor connection or bad fiber could also cause this alarm.
LPR	OC3, OC12, or OC48	164	Low Laser Power (receiver)
MAN	OC3, OC12, or OC48	144	Manual. An operate protection switch command was executed on a facility with the switch mode set to Manual.
MAN-RING	OC48	170	A BLSR ring request has been made manually to switch from working to protection channels.
MTCE	OC3, OC12, or OC48	173	Maintenance. An OC facility has been placed in maintenance service state.
RFI	OC3, OC12, or OC48	176	Remote Failure Indication. The far end has detected an LOS, LOF, or AIS line failure on a facility.

Table A. OCn Facility Alarms/Conditions/Events (cont)

IF ALARM/ CONDITION IS...	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
SECTRCERR	OC48	179	The section trace data (SCNTRCDATA) is the same on both the incoming and outgoing section trace. TRIAIS = Y and SCNSEL = TR1.
SECTRCMF	OC3, OC12, or OC48	187	Section Trace Mismatch. Expected section trace and the incoming section trace are different. Either the section trace is misprovisioned at one end of the SONET section or the intended traffic is not being received.
SWEX-RING	OC48	200	A BLSR span switch exercise, automatic or manual, has failed. The NE that initiated attempted switch exercise failed to receive the appropriate response from the other NE within 100 msecs.
SYNCLEVINFAIL	OC3, OC12, or OC48	204	Synchronization Level Input Failure. NE has received an invalid synchronization message value or synchronization values that are constantly changing.
T-CVL	NEND OCn in RCV direction	220	Coding violations - Line TCA*. Bit Interleaved Parity (BIP) errors
	FEND OCn in RCV direction	220	Coding violations - Line TCA*. Far End Bit Errors (FEBE)
T-CVS	NEND OCn in RCV direction	220	Coding violations - Section TCA*. Bit Interleaved Parity (BIP) errors
T-ESL	NEND OCn in RCV direction	220	Errored seconds - Line TCA*
	FEND OCn in RCV direction	220	Errored seconds - Line TCA*
T-ESS	NEND OCn in RCV direction	220	Errored seconds - Section TCA*
T-SEFS	NEND OCn in RCV direction	220	Severely errored framing seconds TCA*
T-SESL	NEND OCn in RCV direction	220	Severely errored seconds - Line TCA*
	FEND OCn in RCV direction	220	Severely errored seconds - Line TCA*
T-SESS	NEND OCn in RCV direction	220	Severely errored seconds - Section TCA*

Table A. OCn Facility Alarms/Conditions/Events (cont)

IF ALARM/ CONDITION IS...	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
T-UASL	NEND OCn in RCV direction	220	Unavailable seconds - Line TCA*
	FEND OCn in RCV direction	220	Unavailable seconds - Line TCA*
Condition	**Action**		**Description**
ACT	No action		HIF is active; near end or far end
ACTLPBK	No action		Loopback active
AINS	No action		Automatic-In-Service state
BRIDGE-ACT	No action		Bridge on working/protection is active (BLSR)
K1-xx (rcv) where xx=0...255	No action		Received APS K1 byte (Linear APS or BLSR)
K1-xx (trmt) where xx=0...255	No action		Transmit APS K1 byte (BLSR only)
K2-xx (rcv) where xx=0...255	No action		Received APS K2 byte (Linear APS or BLSR)
K2-xx (trmt) where xx=0...255	No action		Transmit APS K2 byte (BLSR only)
STBY	No action		HIF is standby; near end or far end
SYNCLEVIN-( )	No action		Input synchronization message value (0...15)
SYNCLEVOUT-( )	No action		Output synchronization message value (0...15)
Event	**Action**		**Description**
ACTLPBK	No action		Loopback active
AINS	No action		Automatic-In-Service state
FRCDWKSWBK	No action		Protected path forced to switch back to working — near end or far end
FRCDWKSWPR	No action		Forced switch to protection - near end or far end
FRCDWKSWPR-RING	No action		Working path forced to switch to protection (BLSR)
IS-AUTO	No action		Automatic OOS-MA to IS
LOCKOUTOFPR	No action		Lock out of protection — near end or far end
MANWKSWBK	No action		Manual switch back to working — NE or FE
MANWKSWPR	No action		Manual switch to protection — NE or FE
MANWKSWPR-RING	No action		Manual switch of working to protection (BLSR)

Table A. OCn Facility Alarms/Conditions/Events (cont)

Event	Action	Description
SECTRCHG	No action	Section trace changed
SIGDEG	No action	Far end – signal degraded
SIGDEG-RING	No action	BLSR signal degraded (switch reason)
SIGFAIL	No action	Far end – signal fail
SIGFAIL-RING	No action	BLSR signal failure (switch reason)
SYNCLEVINCHG	No action	Synchronization level input change
UNASSIGN	No action	OCm facility is unassigned
WKSWBK	No action	Near end: switch back to working
WKSWBK-RING	No action	Working switched back (BLSR)
WKSWPR	No action	Near end – switch to protection
WKSWPR-RING	No action	Working switched to protection (BLSR)
WTRREVERT	No action	Wait for revert/restore timeout – NE or FE
WTRREVERT-RING	No action	Wait to restore timeout (in revertive mode) (BLSR)
* *TCA = Threshold Crossing Alert*		

Alarm/Condition – AISL

4 Retrieve alarms at the upstream NE [DLP-100].

5 Is there an LOS or LOF alarm on the incoming signal?

If yes, then go to step 164.
If no, then continue to step 6.

6 At the upstream NE, check Line Terminating Equipment (LTE) supporting the facility.

7 Were any problems found with the LTE?

If yes, clear LTE problem using vendor's documentation.
If no, then then continue to step 9.

8 STOP. This procedure is complete.

9 At the far-end NE, is the alarmed OCn facility either unassigned or in maintenance state?

If yes, restore facility to in-service [DLP-501].
If no, contact Customer Service.

10 STOP. This procedure is complete.

Alarm/Condition – ALS

11 ***NOTE:*** *Automatic Laser Shutdown (ALS) is a maintenance safety feature that provides the option of having the transmit laser automatically shut off when Loss-of-Signal (LOS) is detected on the optical receiver. The ALS alarm is active as long as LOS alarm is present*

Do you want to clear LOS alarm at this time?

If yes, then continue to step 12.
If no, then go to step 23.

12 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing the HIF or LIF to avoid service interruption.**

13 At the near-end NE, replace HIF or LIF unit associated with alarmed facility [DLP-101]; then retrieve alarms [DLP-100].

14 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 15.

15 At the far-end NE that terminates the OCn line, replace HIF or LIF unit associated with alarmed facility [DLP-101].

16 Retrieve alarms [DLP-100].

17 Did alarm clear?

If yes, then go to step 19.
If no, test facility per local practice.

18 STOP. This procedure is complete.

19 Retrieve facilities provisioned parameters to see how laser restart is provisioned [DLP-502].

20 Is ALS Mode provisioned Automatic or Manual?

If Automatic, then continue to step 21.
If Manual, then go to step 24.

21 ***NOTE:*** *Note the provisioned value for the Automatic Laser Shutdown Delay parameter.*

Wait for laser to restart (60 to 300 seconds).

22 STOP. This procedure is complete.

23 **NOTE:** *The laser will restart after a 60 to 300 second delay (delay time is defined in the ALS Delay parameter); however, as long as the LOS is present, the laser will shut down again after 1.75 to 2.25 seconds. This shut down restart cycle can be ended by overriding the laser shutdown.*

Do you want to end the shutdown restart cycle?

If yes, go to step 24.
If no, go to step 25.

24 Manually restart the laser [DLP-540].

25 STOP. This procedure is complete.

Alarm/Condition – APSB

26 If alarm is on an LIF in simplex mode, follow procedure for BERL–HT/BERL–LT (steps 114–122).

27 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid service interruption.**

28 Retrieve alarms at the far-end NE [DLP-100].

29 Are there any HIF or LIF alarms?

If yes, resolve alarms per TAP-021.
If no, then continue to step 30.

30 Retrieve alarms at the near-end NE [DLP-100].

31 Are there any HIF or LIF alarms?

If yes, resolve alarms per TAP-021.
If no, then continue to step 32.

32 Retrieve OCn conditions [DLP-100].

33 Is the alarmed OCn facility active (ACT)?

If yes, then continue to step 34.
If no, then go to step 35.

34 Switch service away from alarmed facility [DLP-513].

35 Repeat steps 32 through 34 at the far-end NE that terminates the alarmed OCn span to switch the active side away from the alarmed facility.

36 Place HIF or LIF in maintenance state [DLP-501].

37 **CAUTION: Possibility of service interruption. The following step may interrupt service if not switched to protecting line.**

38 Run diagnostic Phase 15 (SA, K1/K2 APS test) on HIF or LIF carrying alarmed OCn facility [DLP-500]. Perform 5 iterations.

39 Place HIF or LIF back in-service [DLP-501].

40 Did diagnostics pass?

If yes, go to step 42.
If no, then go to step 41.

41 Replace HIF or LIF per DLP-101; then go to step 45.

42 Repeat steps 36 through 39 to diagnose far-end HIF or LIF.

43 Did diagnostics pass?

If yes, then go to step 45.
If no, then continue to step 44.

44 Replace HIF or LIF per DLP-101.

45 Was a protection switch performed on the OCn facility at the near end or far end NE?

If yes, then continue to step 46.
If no, then go to step 47.

46 At near end and/or far end, release protection switching [DLP-545].

47 Retrieve alarms [DLP-100].

48 Did alarms occur again?

If yes, contact Customer Service.
If no, then go to step 49.

49 STOP. This procedure is complete.

Alarm/Condition – APSCM or APSMM

50 Check provisioning of Protection Switching parameters at both ends of the alarmed OCn span [DLP-541].

51 Are the parameters the same at both ends?

If yes, then go to step 55.
If no, then continue to step 52.

52 Change the Protection Switching parameters at the incorrect end [DLP-541].

53 Retrieve alarms [DLP-100].

54 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 55.

55 Retrieve OCn conditions at near-end NE [DLP-100].

56 Is the alarmed OCn facility active (ACT)?

If yes, then continue to step 57.
If no, then go to step 58.

57 Switch service away from alarmed facility [DLP-513].

58 Retrieve OCn conditions at far-end NE [DLP-100].

59 Is the far-end OCn facility active?

If yes, then continue to step 60.
If no, then go to step 61.

60 Switch service away from active OCn facility at far-end [DLP-513].

61 At near-end NE, place HIF or LIF in maintenance state [DLP-501].

62 **CAUTION: Possibility of service interruption. The following step may interrupt service if not switched to protecting line.**

63 Run diagnostic Phase 15 (SA, HIF K1/K2 APS test) on HIF or LIF carrying alarmed OCn facility [DLP-500]. Perform 5 iterations.

64 Did diagnostics pass?

If yes, then continue to step 67.
If no, then go to step 65.

65 **CAUTION: Possibility of service interruption. Adhere to DLP-101 when replacing a plug-in unit to avoid interrupting service.**

66 Replace HIF or LIF per DLP-101; then go to step 69.

67 Place HIF or LIF back in-service [DLP-501].

68 Have diagnostics been run on HIF or LIF at far-end NE?

If yes, then go to step 69.
If no, repeat steps 61 through 67 at far-end NE.

69 Was a protection switch performed on the OCn facility at the near end or far end?

If yes, then continue to step 70.
If no, go to step 71.

70 At near end and/or far end, release protection switching [DLP-545].

71 Retrieve alarms [DLP-100].

72 Did alarms occur again?

If yes, contact Customer Service.
If no, then go to step 73.

73 STOP. This procedure is complete.

Alarm/Condition – APSDFLT (Receive Direction)

74 Determine direct neighbor on receive side (LG1 side) [DLP-560].

75 Log on to direct neighbor [DLP-117] and retrieve BLSR ring parameters [DLP-543].

76 Is BLSR mode enabled on direct neighbor NE?

If yes, then go to step 80.
If no, then continue to step 77.

77 Change BLSR mode on neighbor node to enabled [DLP-543].

78 Retrieve alarms [DLP-100].

79 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 80.

80 Retrieve BLSR Ring parameters and determine ID of neighbor node [DLP-543].

81 Retrieve BLSR Automatic Sequence Map and note NEs in the BLSR ring [DLP-564].

82 Is LG1 neighbor node ID used by another node on the ring?

If yes, then continue to step 83.
If no, then go to step 86.

83 Change node ID of neighbor node [DLP-543].

84 Retrieve alarms [DLP-100].

85 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 86.

86 Check the neighbor node for transmit APS default alarms [DLP-100].

87 Are any transmit APS alarms reported on neighbor node?

If yes, go to step 89 and clear APSDFLT alarm in transmit direction.
If no, contact Customer Service.

88 STOP. This procedure is complete.

Alarm/Condition – APSDFLT (Transmit Direction)

89 Retrieve BLSR Ring parameters and check status of Automatic Map Generation parameter [DLP-543].

90 Is Automatic Map Generation parameter enabled?

If yes, then continue to step 91.
If no, then go to step 96.

91 Check for BLSR ring alarms [DLP-100].

92 Are any of the following BLSR alarms being reported: BLSRCONN, BLSRPROV, BLSROUTOFSYNC, RINGMAPPROV, or DUPNODEID?

If yes, go to TAP-058.
If no, then continue to step 93.

93 ***NOTE:*** *Automatic map generation cannot take place until the NE is able to communicate with both of its neighbors. In order to clear the APSDFLT alarm, arbitrary neighbor nodes will be created in the manual sequence map. After communications with the neighbor nodes are re-established, automatic map generation will discover the neighbor node IDs. As long as automatic map generation is enabled, the neighbor node IDs created in the manual sequence map will be ignored.*

Create an entry for the local NE in the manual sequence map using arbitrary neighbor node IDs [DLP-542].

94 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

95 STOP. This procedure is complete.

96 Create a ring map entry for the local node [DLP-542].

97 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

98 STOP. This procedure is complete.

Alarm/Condition – APSIMPROP

99 Retrieve BLSR Automatic Sequence Map and check for duplicate Node IDs [DLP-564].

100 Were any Node IDs duplicated?

If yes, change one of the duplicated Node IDs [DLP-543].
If no, then go to step 102.

101 STOP. This procedure is complete.

102 Are there any other OC48 alarms?

If yes, return to step 3 and clear other OC48 facility alarms.
If no, then continue to step 103.

103 Check ring configuration for valid 2-Fiber BLSR NEs.

104 Contact Customer Service.

105 STOP. This procedure is complete.

Alarm/Condition – APSINCON

106 Check for other OC48 facility alarms [DLP-100].

107 Are there any other OC48 facility alarms?

If yes, return to step 3 and clear other OC48 facility alarms.
If no, then continue to step 108.

108 Check for equipment alarms [DLP-100].

109 Are there any equipment alarms?

If yes, then go to TAP-021.
If no, contact Customer Service.

110 STOP. This procedure is complete.

Alarm/Condition – APSNODEIDMM

111 Retrieve BLSR Automatic Sequence Map and check for duplicate Node IDs [DLP-564].

112 Were any Node IDs duplicated?

If yes, change one of the duplicate Node ID [DLP-543].
If no, contact Customer Service.

113 STOP. This procedure is complete.

Alarm/Condition – BERL-HT or BERL-LT

114 Test fiber facility per local practice. Correct problems, if any.

115 Was problem found and corrected on facility?

If yes, STOP. This procedure is complete.
If no, then continue to step 116.

116 **CAUTION: Possibility of service interruption. Adhere to DLP-101 in the following steps when replacing a plug-in unit to avoid interrupting service.**

117 Replace near-end HIF or LIF associated with alarmed facility [DLP-101].

118 Retrieve alarms [DLP-100].

119 Did alarm clear (may take several minutes to clear)?

If yes, STOP. This procedure is complete.
If no, then continue to step 120.

120 Replace far-end HIF or LIF associated with alarmed facility [DLP-101]; then retrieve alarms [DLP-100].

121 Did alarm clear (may take several minutes to clear)?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

122 STOP. This procedure is complete.

Alarm/Condition – FAILTOSW

123 Retrieve alarms at far end of the alarmed OCn span [DLP-100].

124 Are there any HIF or LIf alarms?

If yes, then go to TAP-021.
If no, then continue to step 125.

125 Are any of the following alarms present at the far end NE: APSCM, FRCD, LOCKOUTOFPR, LOS, or LOF?

If yes, return to step 3 and clear other OCn facility alarms.
If no, then continue to step 126.

126 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing a plug-in unit to avoid service interruption.**

127 At the near end NE, replace HIF or LIF associated with alarmed facility; then retrieve alarms [DLP-100].

128 Did alarms clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 129.

129 Replace the adjacent HIF or LIF per DLP-101; then retrieve alarms [DLP-100].

130 Did alarms clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

131 STOP. This procedure is complete.

Alarm/Condition – FAILTOSW-RING

132 Check for other OC48 facility alarms [DLP-100].

133 Are there any other OC48 facility alarms?

If yes, return to step 3 and clear other OC48 facility alarms.
If no, then continue to step 134.

134 Check for equipment alarms [DLP-100].

135 Are there any equipment alarms?

If yes, then go to TAP-021.
If no, contact Customer Service.

136 STOP. This procedure is complete.

Alarm/Condition – FEPRLF

137 Retrieve alarms at far end of the alarmed OCn span [DLP-100].

138 Are any equipment alarms (especially HIF or LIF) being reported?

If yes, then go to TAP-021.
If no, then continue to step 139.

139 Are any other OCn alarms reported?

If yes, return to step 3 and clear other OCn facility alarms.
If no, contact Customer Service.

140 STOP. This procedure is complete.

Alarm/Condition – FRCD-RING

141 **CAUTION: Possibility of service interruption. A forced or locked-out switch may cause a service interruption if the active facility fails and a switch is required.**

142 To clear alarm, release forced switch request [DLP-545].

143 STOP. This procedure is complete.

Alarm/Condition – FRCD, LOCKOUTOFPR or MAN

144 **CAUTION: Possibility of service interruption. A forced or locked-out switch may cause a service interruption if the active facility fails and a switch is required.**

145 To clear alarm, release facility switch request [DLP-545].

146 STOP. This procedure is complete.

Alarm/Condition – INHEX-RING

147 To clear alarm, allow automatic BLSR ring switch exerciser [DLP-544].

148 STOP. This procedure is complete.

Alarm/Condition – INHPMREPT

149 To clear alarm, allow PM reporting on facility [DLP-510].

150 STOP. This procedure is complete.

Alarm/Condition – LINENA

151 Retrieve OCn alarms and conditions [DLP-100].

152 Check for the following conditions: AISL, APSB, BER-HT, BERL-LT, LOF, or LOS. Do any of these conditions exist?

If yes, refer to Table B.
If no, then continue to step 153.

Table B. Condition Selection

IF CONDITION IS...	THEN GO TO...
AISL	Step 4
APSB	Step 26
BERL-HT or BERL-LT	Step 114
LOF or LOS	Step 164

153 Retrieve alarms at the far-end NE [DLP-100].

154 Are there any HIF/LIF alarm indications at the far-end NE?

If yes, then go to TAP-021.
If no, then continue to step 155.

155 Retrieve alarms at the near-end NE [DLP-100].

156 Are there any HIF/LIF alarm indications at the near-end NE?

If yes, then go to TAP-021.
If no, contact Customer Service if problem persists.

157 STOP. This procedure is complete.

Alarm/Condition – LOCKOUT-LOWR

158 **CAUTION: Possibility of service interruption. A forced or locked-out switch may cause a service interruption if the active facility fails and a switch is required.**

159 To clear alarm, release lockout request [DLP-545].

160 STOP. This procedure is complete.

Alarm/Condition – LOCKOUT-LPS

161 **CAUTION: Possibility of service interruption. A forced or locked-out switch may cause a service interruption if the active facility fails and a switch is required.**

162 To clear alarm, release lockout request [DLP-545].

163 STOP. This procedure is complete.

Alarm/Condition – LOF, LOS, or LPR

164 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing the HIF or LIF to avoid service interruption.**

165 Replace HIF or LIF unit associated with alarmed facility per DLP-101; then retrieve alarms [DLP-100].

166 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 167.

167 At the far-end NE that terminates the OCn line, replace HIF or LIF unit associated with alarmed facility per DLP-101; then retrieve alarms.

168 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, test facility per local practice.

169 STOP. This procedure is complete.

Alarm/Condition – MAN-RING

170 **CAUTION: Possibility of service interruption. A forced or locked-out switch may cause a service interruption if the active facility fails and a switch is required.**

171 To clear alarm, release manual switch request [DLP-545].

172 STOP. This procedure is complete.

Alarm/Condition – MTCE

173 **CAUTION: Possibility of service interruption. The facility should not be left in the maintenance state for an unnecessary length of time since it cannot carry traffic while in the state.**

174 To clear alarm, return the facility to in-service [DLP-502].

175 STOP. This procedure is complete.

Alarm/Condition – RFI

176 Retrieve alarms at the far end NE [DLP-100].

177 Go to IXL-001 and find the appropriate TAP to use to resolve the alarm(s).

178 STOP. This procedure is complete.

Alarm/Condition – SECTRCERR

179 Check for a looped OC48 signal in network.

180 Was a looped OC48 signal found?

If yes, release loopback [DLP-523].
If no, then continue to step 181.

181 Retrieve outgoing and incoming section trace data [DLP-547] and check this data against office records.

182 Is section trace data correct?

If yes, go to step 183.
If no, go to step 185.

183 Contact Customer Service.

184 STOP. This procedure is complete.

185 If outgoing data is not correct, correct section trace provisioning at near end NE and if incoming data is not correct, correct section trace provisioning at far end NE [DLP-547].

186 STOP. This procedure is complete.

Alarm/Condition – SECTRCMF

187 Do you want section trace enabled?

If yes, then go to step 189.
If no, disable monitoring of the section trace [DLP-546].

188 STOP. This procedure is complete.

189 Retrieve received incoming section trace information and provisioned incoming (expected) section trace information [DLP-547].

190 From the response, compare the provisioned incoming (expected) value with the received incoming value. From office records, determine which component value is wrong.

If Provisioned Incoming, then continue to step 191.
If Received Incoming, then go to step 193.

191 Change the provisioned incoming value to match the incoming section tracer [DLP-547].

192 STOP. This procedure is complete.

193 Log on to the far-end NE that is supposed to terminate this OCn facility.

194 At the far end, retrieve provisioned expected section trace information [DLP-547].

195 Is the Trace Format parameter set to TR1 (Provisionable Format) and is the Provisioned Outgoing setting the same as the value expected at the near end (0...255)?

If yes, then continue to step 196.
If no, then go to step 198.

196 Troubleshoot facility per local procedures.

NOTE: *An incorrect cross-connection in the facility is the most probable cause.*

197 STOP. This procedure is complete.

198 At the far-end NE, change the section trace Provisioned Outgoing value to match the section trace Provisioned Incoming value at the near end [DLP-547].

199 STOP. This procedure is complete.

Alarm/Condition – SWEX-RING

200 Are there any BLSR ring alarms [DLP-100]?

If yes, then go to TAP-058 and clear BLSR ring alarms.
If no, go to step 201.

201 Are there any other OC48 facility alarms [DLP-100]?

If yes, return to step 3 and clear other OC48 facility alarms.
If no, then continue to step 202.

202 Are there any equipment alarms [DLP-100]?

If yes, then go to TAP-021.
If no, contact Customer Service.

203 STOP. This procedure is complete.

Alarm/Condition – SYNCLEVINFAIL

204 Retrieve current OCn synchronization conditions [DLP-100].

205 Note the number following **SYNCLEVIN**.

NOTE: *The number following SYNCLEVIN is the synchronization status message (expressed as a decimal number). This message is contained in the S1 portion (bits 5-6-7-8) of the S1/Z1 byte in the STS frame transport overhead.*

206 Is the synchronization status message a valid value (0, 1, 4, 7, 10, 12, 13, 14, or 15)?

If yes, then continue to step 207.
If no, then go to step 214.

207 In the first column of Table C, find the number (synchronization status message) noted in step 205.

NOTE: *The other columns define the quality level and the synchronization traceability that correspond to that synchronization status message.*

Table C. Interpretation of SYNCLEVIN Message Values

SYNCHRONIZATION STATUS MESSAGE	QUALITY LEVEL		SYNCHRONIZATION TRACEABILITY
	1ST GENERATION (V1)	2ND GENERATION (V2)	
0	2	2	Traceability Unknown
1	1	1	Stratum 1 Traceable
4	N/A	4	Transit Node Clock Traceable
7	3	3	Stratum 2 Traceable
10	4	6	Stratum 3 Traceable
12	5	7	Minimum Clock Traceable
13	N/A	5	Stratum 3E Traceable
14	User assignable	User assignable	Reserved for network sync
15	7	9	Don't use for synchronization

208 Is the quality level 1, 2, 3, or 4?

If no, then continue to step 209.
If yes, then go to step 211.

209 Network synchronization provisioning is probably not correct. Contact Customer Service.

210 STOP. This procedure is complete.

211 Retrieve current OCn synchronization conditions again [DLP-100].

212 Is the synchronization message value the same as it was when you checked it the first time?

If yes, contact Customer Service.
If no, the synchronization value is changing; go to step 214.

213 STOP. This procedure is complete.

214 Retrieve alarms [DLP-100].

215 Are there other alarms on OCn facility?

If yes, return to step 3 and clear other OCn facility alarms.
If no, then continue to step 216.

216 Are there any equipment alarms?

If yes, then go to TAP-021.
If no, then continue to step 217.

217 Perform steps 214 through 216 at the adjacent NE (the NE that is transmitting data for the alarmed facility).

218 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

219 STOP. This procedure is complete.

Alarm/Condition – T-xxx

220 ***NOTE:*** *A threshold crossover alarm has been generated because one of the performance parameters listed in Table D exceeded the provisioned value. As a default, these conditions are not reported as an alarm, but as an event, unless the attribute has been changed to minor (MN), major (MJ), or critical (CR).*

Retrieve OCn alarms and conditions [DLP-100]; then go to step 221.

Table D. OC3, OC12, and OC48 PM Thresholds

MONITOR TYPE	FACILITY	FACTORY DEFAULT		RANGE	DESCRIPTION
		15-MIN	1-DAY		
BERL-HT	All OCn	4		3...5	Bit Error Ratio Line – High threshold (SFBER)
BERL-LT	All OCn	7		5...9	Bit Error Ratio Line – Low threshold (DGBER)
CVL	OC3	1328	13288	1...4,294,967,295	Coding violation count (line)
	OC12	5315	53150	1...4,294,967,295	
	OC48	21260	212602	1...4,294,967,295	
CVS	OC3	1344	13437	1...4,294,967,295	Coding violation count (section)
	OC12	5375	53748	1...4,294,967,295	
	OC48	21499	214991	1...4,294,967,295	
DSESL	OC3	2500		1...65535	Number of coding violations to make one SESL
	OC12	10000		1...65535	
	OC48	40300		1...65535	
DSESS	OC3	2500		1...65535	Number of coding violations to make one SESS
	OC12	8800		1...65535	
	OC48	23100		1...65535	
ESL	OC3	20	200	1...65535	Line Errored Seconds
	OC12	60	600	1...65535	
	OC48	180	1800	1...65535	
ESS	OC3	20	200	1...65535	Section Errored Seconds
	OC12	60	600	1...65535	
	OC48	180	1800	1...65535	
SEFS	All OCn	2	17	1...65535	Severely Errored Framing Seconds – OOFS/COFAS

Table D. OC3, OC12, and OC48 PM Thresholds (cont)

MONITOR TYPE	FACILITY	FACTORY DEFAULT		RANGE	DESCRIPTION
		15-MIN	1-DAY		
SESL	All OCn	3	7	1...65535	Line Severely Errored Seconds
SESS	All OCn	3	7	1...65535	Section Severely Errored Seconds
UASL	All OCn	10	10	1...65535	Line Unavailable Seconds

221 Are there any other facility alarms (besides T-xxx)?

If yes, return to step 3 and clear other OCn facility alarms first.
If no, then go to step 223.

222 STOP. This procedure is complete.

223 Is the condition severe enough to warrant unit replacement?

If yes, then go to step 225.
If no, record the alarm as an event.

224 STOP. This procedure is complete.

225 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing the HIF to avoid service interruption.**

226 From the work view opened in step 220, note location of T–xxx in Location column.

227 Is location of T-xxx condition near end or far end?

If near end, then continue to step 228.
If far end, then go to step 229.

228 ***NOTE:*** *The near end is detecting a problem on the receive (facility) side. Problem is most likely at far-end equipment or on a facility.*

Replace far-end HIF or LIF associated with alarmed facility per DLP-101; then go to step 230.

229 ***NOTE:*** *The far end is detecting a problem on the receive (facility) side. Problem is most likely at near-end equipment or on a facility.*

Replace near-end HIF or LIF associated with alarmed facility per DLP-101; then continue to step 230.

230 Retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

231 Did PM errors stop?

If yes, then STOP. This procedure is complete.
If no, troubleshoot facility per local practice.

232 STOP. This procedure is complete.

TAP-031
Clear Remote (RMT) Alarm

Purpose

Provides a procedure for clearing a remote alarm.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Do you know which NE is generating the alarm? If yes, go to step 4. If no, go to step 2.
2	Retrieve alarms for each NE in the domain [DLP-100].
3	Identify the alarmed NE.
4	Attempt to log on to the remote NE reporting the alarm [DLP-117].
5	Were you able to log on? If yes, go to step 7. If no, go to step 6.
6	Go to the remote site, analyze visual indicators, and resolve alarm (refer to TAP-010).
7	Identify alarm using 1301 NMX and resolve alarm, or enlist assistance from craftsperson at remote site to perform corrective actions that cannot be performed remotely (refer to TAP-001).
8	STOP. This procedure is complete.

TAP-032
Clear LLSDCC (EOC) Alarm

Purpose

Provides a procedure for clearing a LLSDCC (EOC) alarm on OCn facilities.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

STEP	PROCEDURE
1	Retrieve alarms and note which facility is carrying the alarmed EOC [DLP-100].
2	**NOTE:** *The Component column (aid) in the Alarms work view contains the facility carrying the alarmed LLSDCC EOC (Embedded Overhead Channel). The facility identified could be LG1 (Line Group 1), LG2 (Line Group 2) or DGx-n (Drop Group x, line n where x = 1...4, n = 1...4) or DGxm-n (Drop Group x, side m, line n where x=1...4, m=A, B, n = 1...4).* **NOTE:** *Other alarms on facility should be cleared first since they may affect EOC communications.* From office records, determine the facility type (i.e., OC3, OC12, or OC48) that is carrying the alarmed EOC. Also, look for other alarms on the facility.
3	Are there any other OC3, OC12, or OC48 alarms? If yes, go to TAP-029. If no, go to step 4.
4	**NOTE:** *Conflict may exist in LLSDCC Side Role (l2side) parameter entries at the local NE and the far-end NE that terminates the alarmed EOC. A proper Side Role parameter entry at both NEs must be made for each to establish EOC communication and retire EOC alarm. The Side Role parameter value setting for one end of the link must be User Side, and the other end of the link must be set to Network Side for proper operation. Other LLSDCC parameters should be the same at the two NEs. Also, the primary state of the LLSDCC entity must be in-service at both ends of the link.* **NOTE:** *If EOC communication is unavailable, remote logon to the remote NE may not be possible. You may have to go to the remote NE and log on to retrieve and modify the LLSDCC parameters.*

Check the service state and provisioning of the Side Role parameter on LG1 side and LG2 side:

NOTE: *EOC may be on either line group or on an OCn drop group.*

a. In the scope pane, expand System; then expand protocol and select DCC-Lower Layer.

b. In the result pane, right-click LG1 to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. Note the service state and provisioning of the Side Role parameter on LG1 side.

e. Close work view and repeat from step 4a for LG2 side.

5 Are both ends in service and is the Side Role parameter set to User Side on one end and to Network Side on the other?

If yes, go to step 9.
If no, go to step 6.

6 On the Provision Parameters work view, change the service state and/or Side Role parameter:

a. To change the service state, select In Service from the Service State drop-down list.

a. To change the Side Role, select User Side or Network Side from the Side Role drop-down list.

b. On the toolbar, select Submit icon; then close work view.

7 Retrieve alarms [DLP-100].

8 Did the EOC alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 9.

9 All probable causes have been considered. Look for other (obscure) alarm conditions which may indirectly be causing this alarm [TAP-001] or contact Customer Service [TNG-505].

10 STOP. This procedure is complete.

TAP-033
Clear SML Facility Alarm

Purpose

Provides procedures for clearing Synchronous Maintenance Link (SML) facility alarms.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Retrieve alarms [DLP-100].
2	Are there any NEP alarms? If yes, go to TAP-021. If no, go to step 3.
3	Locate the alarm or condition in Table A; then go to step indicated to clear it.

Table A. SML Facility Alarms

ALARM/CONDITION	REASON FOR ALARM	STEP
AIS	Alarm Indication Signal. All ones are sent downstream to notify other NEs of a failure in the signal path.	4
AISYEL	Alarm Indication Signal – Yellow. A status condition that alerts upstream equipment that an AIS has been received in the downstream equipment.	6
BER-HT	Bit Error Ratio – High Threshold. The ratio of the number of bits in error to the total number of bits transmitted during a measured period has exceeded the threshold.	12
LOF	Loss-of-Frame. An excessive amount of out-of-frame occurrences took place on the incoming signal.	23
LOS	Loss-of-Signal. A complete loss-of-signal, all-zeros-pattern, or no physical layer has been received.	12

Table A. SML Facility Alarms (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
MTCE	Maintenance. SML facility is in maintenance state.	34
YEL	Yellow. The NE has received a notification from the SML link that there is an upstream failure. It indicates that the far-end equipment has detected a receive failure. Far-end equipment generates a yellow alarm when it detects a variety of conditions.	12

Alarm – AIS

4 The problem is not in this NE. Check for alarms at interconnected equipment.

5 STOP. This procedure is complete.

Alarm – AISYEL

6 Verify SML wire-wrap connections on backplane (see Figure 1).

7 Are connections good?

If yes, go to step 8.
If no, go to step 10.

8 Suspect equipment or facility problems (refer to TAP-001).

9 STOP. This procedure is complete.

10 Correct the connection per Figure 1.

11 STOP. This procedure is complete.

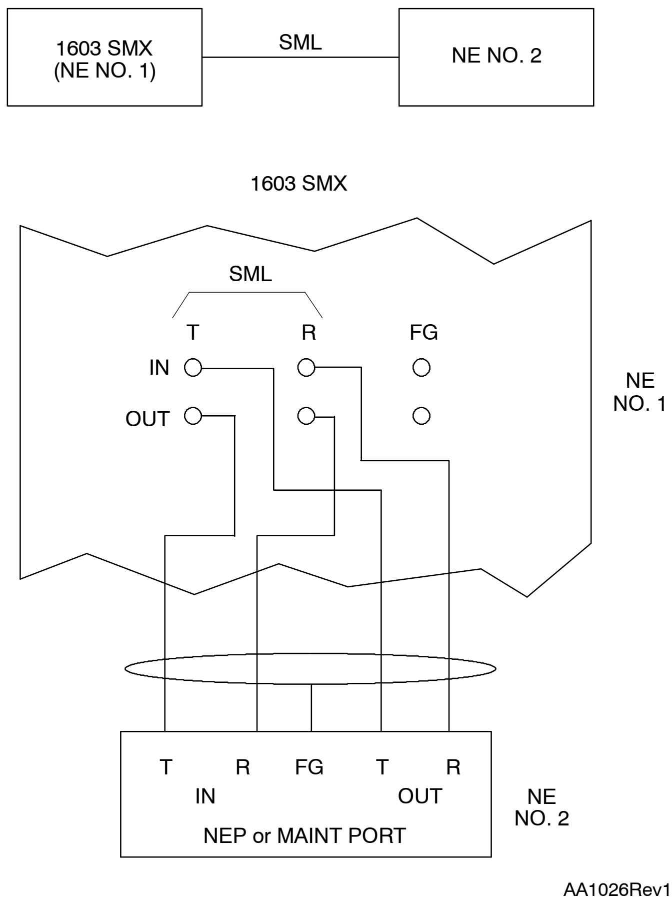


Figure 1. SML Wiring Interface

Alarm – BER-HT, LOS, and YEL

12 Are you trying to clear a BER-HT alarm?

If yes, then go to step 13.
If no, then go to step 17.

13 Retrieve and verify equalization at other NE [DLP-531].

14 Is equalization distance correct?

If yes, then go to step 17.
If no, then go to step 15.

15 Change equalization distance [DLP-531]; then retrieve alarms [DLP-100].

16 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 17.

17 Verify wire-wrap connections on backplane and correct if necessary (see Figure 1).

18 Is the connection good?

If yes, go to step 21.
If no, go to step 19.

19 Correct the connection per Figure 1.

20 STOP. This procedure is complete.

21 The problem is at the other NE terminating the SML link. Check for alarms at interconnected equipment. Troubleshoot problem at the source.

22 STOP. This procedure is complete.

Alarm – LOF

23 Verify wiring at NEP SML wire-wrap connections on backplane (per Figure 1).

24 Is the connection good?

If yes, go to step 27.
If no, go to step 25.

25 Correct the connection per Figure 1.

26 STOP. This procedure is complete.

27 Check provisioning of Line Code and Format parameters at the two NEs terminating the SML link to ensure agreement on both ends [DLP-502].

28 Are parameters correct?

If yes, then go to step 32.
If no, then go to step 29.

29 Change parameters so they are the same at both NEs [DLP-502].

30 Retrieve alarms [DLP-100].

31 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 32.

32 The problem is at the other NE terminating the SML link. Check for alarms at interconnected equipment. Troubleshoot problem at the source.

33 STOP. This procedure is complete.

Alarm – MTCE

34 To clear the alarm, place the facility back in-service [DLP-501].

35 STOP. This procedure is complete.

TAP-034
Clear STS (STS1, STS3c, or STS12c) Path Alarm

Purpose

Provides procedures for clearing STS1, STS3c, or STS12c path alarms.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	**NOTE:** *For STS path alarms, supporting equipment and facilities are suspected first.* Perform steps 2 through 8 at each NE in the network before proceeding to step 9.
2	Retrieve alarms [DLP-100].
3	Are there any equipment alarms? If yes, then go to step 4. If no, then go to step 6.
4	**NOTE:** *All unit alarms are indicated on the COA unit by severity level (CR [Critical], MJ [Major], or MN [Minor]). If there is a COA CONTCOM and an NEP alarm, resolve the COA alarm first.* Identify the alarmed unit with the highest severity and go to TAP-021 to clear equipment alarm(s).
5	STOP. This procedure is complete.
6	Are there any OCn facility alarms? If yes, go to TAP-029. If no, then continue to step 7.
7	Are there any EC1 facility alarms? If yes, go to TAP-022. If no, then continue to step 8.

8 Are there any T3 (DS3) facility alarms?

If yes, go to TAP-043.
If no, then continue to step 9.

9 Retrieve STS alarms [DLP-100].

10 Is Location identified on the Alarms work view?

If yes, then continue to step 11.
If no (NEND is implied), then go to step 13.

11 Is Location = FEND or NEND?

If FEND, then continue to step 12.
If NEND, then go to step 13.

12 Go to far-end NE where STS path is dropped or terminated; then return to step 2.

13 Locate the alarm or condition you want to clear in Table A; then go to step indicated to clear it.

NOTE: *The same alarm may be generated by an STS1, STS3c, or STS12c path; however, the procedure for clearing the alarm may be different for each path type. Therefore, be sure you go to the step referenced for the path type generating the alarm.*

Table A. STS Path Alarms/Conditions/Events

IIF ALARM/ CONDITION IS...	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
AISP (rcv & trmt)	Any STS path	14	Path Alarm Indication Signal. A failure has occurred on an upstream NE. AIS has been inserted into an STS path so that downstream cross-connect selectors are switched away from the failure, an unterminated path, or a removed facility.
BERP-HT (rcv & trmt)	Any STS path	29	Path Bit Error Ratio-High Threshold. The ratio of the number of bits in error to the number of bits received exceeds a threshold setting of 10^{-4}.
BERP-LT (rcv & trmt)	Any STS path	29	Path Bit Error Ratio-Low Threshold. A bit error ratio exceeds a threshold setting between 10^{-5} and 10^{-9}.
BLSRPATHNA	Any STS path	35	BLSR path is not available due to a failure, for example, path AIS, UNEQ, PLM, or BERs.

Table A. STS Path Alarms/Conditions/Events (cont)

IIF ALARM/ CONDITION IS...	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
BRIDGE	Any STS path	44	Traffic is bridged on working or protection paths (BLSR).
CONCAT	Any STS path	47	Concatenation Mismatch. A payload type was detected that is different than the payload type provisioned.
ETFAIL	Any STS path	60	Extra Traffic Failed. The drop side STS path is being squelched (i.e., AIS has been inserted in the drop direction. This occurs in a BLSR ring due to BLSR extra traffic preemption. It is normal to have this alarm during BLSR ring failures.
FRCD	Any STS path	65	A forced path switch has been performed on a ring path selector from the line group specified in the alarm message or response.
INHPMREPT	Any STS path	68	Inhibit PM Reports. Autonomous reporting of performance monitoring data has been inhibited on the STS path.
LOCKOUT	Any STS path	65	A locked-out path switch has been performed on a ring path selector from the line group specified in the alarm message or response.
LOMF	STS1 path	70	Loss of Multiframe. The H4 bit value is not received from the far-end STS1 path termination. A missing network cross-connection or misprovisioning could cause this alarm.
LOP	STS1 path in receive direction	78	Loss of Pointer. A valid pointer value cannot be obtained for the Synchronous Payload Envelope (SPE) in the receive direction.
	STS1 path in transmit direction	89	A valid pointer value cannot be obtained for the SPE in the transmit direction. This can occur on a USRLAN STS1 path (LIF901) or for a DS3 payload on the following LIF units: LIF301, LIF501, LIF701, or LIFD01.
	STS3c or STS12c path in receive and transmit direction	94	A valid pointer value cannot be obtained for the STS3c or STS12c Synchronous Payload Envelope (SPE).

Table A. STS Path Alarms/Conditions/Events (cont)

IIF ALARM/ CONDITION IS...	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
MAN	Any STS path	110	A manual path switch has been performed on a ring path selector from the line group specified in the alarm message or response.
PATHSEL	Any STS path	14	Path Selector. Problems on both rings caused the ring path selector to fail and interrupt traffic. The following conditions are probable causes: an upstream failure has occurred; a facility has been removed or is unassigned; or STS cross-connections in both paths are not in place.
PDI	STS1 path in receive direction	112	Path Defect Indication. An upstream NE has detected a defect in either a VT, DS3, or other payload that was mapped into a Synchronous Payload Envelope (SPE). When the NE detects the defect, it inserts a Payload Defect Indication (PDI) value into the C2 byte.
	STS1 path in transmit direction	119	An NE has detected a defect in a DS3 payload that was mapped into Synchronous Payload Envelope (SPE). A PDI value is inserted into the C2 byte.
	STS3c or STS12c path in receive or transmit direction	124	An upstream NE has detected a defect in a payload that was mapped into an STS Synchronous Payload Envelope (SPE). When the NE detects the defect, it inserts a Payload Defect Indication (PDI) value into the C2 byte.

Table A. STS Path Alarms/Conditions/Events (cont)

IIF ALARM/ CONDITION IS...	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
PLM	STS1 path in receive direction	127	Payload Label Mismatch. The content of the C2 byte is inconsistent or invalid. The following conditions are probable causes: the incoming payload type is incorrect due to network routing problems; the expected STS signal label is provisioned incorrectly; or a Payload Label Mismatch (PLM) value is present in the C2 byte.
	STS1 path in transmit direction	134	A payload label mismatch has been detected in a DS3 payload, or on a USRLAN LIF901 STS1 path.
	STS3c path (rcv or trmt)	139	The content of the C2 byte is inconsistent or invalid. The following conditions are probable causes: the incoming payload type is incorrect due to network routing problems; the expected STS signal label is provisioned incorrectly; or a Payload Label Mismatch (PLM) value is present in the C2 byte.
	STS12c path (rcv or trmt)	146	
PROTNA	Any STS path	14	Protection Not Available. A problem on one ring path may cause service interruption if an active ring path fails. The following conditions are probable causes: an upstream failure has occurred; a facility has been removed or unassigned; or STS cross-connections in both paths are not in place.
RFI	Any STS path	153	Remote Failure Indication. A failure has been detected along the downstream STS path.
RFIMM	Any STS path	156	Remote Failure Indication Mismatch. An HIF or LIF has received 1-bit RDI when 3-bit ERDI was enabled or 3-bit ERDI was received when 3-bit ERDI was disabled.
SQUELCH (rcv and trmt)	Any STS path	160	Squelch may happen whenever a BLSR failure occurs. This alarm indicates that traffic is being overwritten by AIS.
TIM	STS1 or STS3c or STS12c path	162	Trace Identifier Message defect. The expected STS path tracer and the incoming path tracer are different. This indicates that the path trace is misprovisioned at either end of the path or the intended STS traffic is not being received.
T-CVP	Any STS path	179	Coding Violations — Path TCA. Bit Interleaved Parity (BIP) errors (NEND RCV or FEND RCV)

Table A. STS Path Alarms/Conditions/Events (cont)

IIF ALARM/ CONDITION IS...	GENERATED BY...	GO TO STEP...	REASON FOR ALARM
T-ESP	Any STS path	179	Errored Seconds – Path Threshold Crossing Alert (TCA). (NEND RCV or FEND RCV)
T-NPJCDET	Any STS path	179	Negative Pointer Justification Count Detected TCA
T-NPJCGEN	Any STS path	179	Negative Pointer Justification Count Generated TCA
T-PPJCDET	Any STS path	179	Positive Pointer Justification Count Detected TCA
T-PPJCGEN	Any STS path	179	Positive Pointer Justification Count Generated TCA
T-PJCSDET	Any STS path	179	Pointer Justification Count Seconds Detected TCA
T-PJCSGEN	Any STS path	179	Pointer Justification Count Seconds Generated TCA
T-PJCSDIFF	Any STS path	179	Pointer Justification Count Difference TCA
T-SESP	Any STS path	179	Severely Errored Seconds – Path TCA (NEND RCV or FEND RCV)
T-UASP	Any STS path	179	Unavailable Seconds – Path TCA (NEND RCV or FEND RCV)
UNEQ	Any STS path (rcv or trmt)	260	The incoming C2 byte was 0 (unequipped). The most likely cause of this alarm is a missing or incorrect STS level cross-connect upstream.
Condition	**Action**		**Description**
ERDI-xxx where xxx = 3 bit RDI value	No action		Enhanced remote defect indication (3 bit RDI)
LCD	No action		Loss of cell delineation
SIGLBL-xxx (RCV) where xxx = 1...255	No action		Received path signal label. xxx is the code received in the C2 byte.
SIGLBL-xxx (TRMT) where xxx = 1...255	No action		Transmitted path signal label. xxx is the code transmitted in the C2 byte.
If STS1 path is connected to a ring selector, the following non-alarmed conditions are added.			
PROTECTED-ACT	No action		Protected path is active
PROTECTING-ACT	No action		Protecting path is active
PROTECTED-ALL	No action		Protected path conditions (TL1 input only)

Table A. STS Path Alarms/Conditions/Events (cont)

Condition	Action	Description
PROTECTING-ALL	No action	Protecting path conditions (TL1 input only)
PROTECTED-BLSRFAIL	[1]	Protected path fails due to BLSR
PROTECTING-BLSRFAIL	[1]	Protecting path fails due to BLSR
PROTECTED-DG1/DG1A/DG1B	No action	Protected path is Drop Group 1, Drop Group 1A, or Drop Group 1B
PROTECTING-DG1/DG1A/DG1B	No action	Protecting path is Drop Group 1, Drop Group 1A, or Drop Group 1B
PROTECTED-DG2/DG2A/DG2B	No action	Protected path is Drop Group 2, Drop Group 2A, or Drop Group 2B
PROTECTING-DG2/DG2A/DG2B	No action	Protecting path is Drop Group 2, Drop Group 2A, or Drop Group 2B
PROTECTED-DG3/DG3A/DG3B	No action	Protected path is Drop Group 3, Drop Group 3A, or Drop Group 3B
PROTECTING-DG3/DG3A/DG3B	No action	Protecting path is Drop Group 3, Drop Group 3A, or Drop Group 3B
PROTECTED-DG4/DG4A/DG4B	No action	Protected path is Drop Group 4, Drop Group 4A, or Drop Group 4B
PROTECTING-DG4/DG4A/DG4B	No action	Protecting path is Drop Group 4, Drop Group 4A, or Drop Group 4B
PROTECTED-FAIL	[2]	Protected path fails
PROTECTING-FAIL	[2]	Protecting path fails
PROTECTED-FRCD	[2]	Forced switch requested on protected path
PROTECTING-FRCD	[2]	Forced switch requested on protecting path
PROTECTED-LG1	No action	Protected path is Line Group 1
PROTECTING-LG1	No action	Protecting path is Line Group 1
PROTECTED-LG2	No action	Protected path is Line Group 2
PROTECTING-LG2	No action	Protecting path is Line Group 2
PROTECTED-LOCKOUT	[2]	Protected path is lockout of protection
PROTECTING-LOCKOUT	[2]	Protecting path is lockout of protection
PROTECTED-MAN	[2]	Manual switch requested on protected path

Table A. STS Path Alarms/Conditions/Events (cont)

Condition	Action	Description
PROTECTING-MAN	[2]	Manual switch requested on protecting path
PROTECTED-PDI	[2]	Protected path has PDI
PROTECTING-PDI	[2]	Protecting path has PDI
PROTECTED-RFI	[2]	Protected path has RFIP
PROTECTING-RFI	[2]	Protecting path has RFIP
PROTECTED-STBY	No action	Protected path is in standby
PROTECTING-STBY	No action	Protecting path is in standby
PROTECTED-UNEQ	[2]	Protected path is unequipped
PROTECTING-UNEQ	[2]	Protecting path is unequipped
Event	**Action**	**Description**
BUERR	No action	RING: STS1 Bus (STAR) failure; reported as switch reason
FRCDWKSWBK	No action	Protected path forced switch back
FRCDWKSWPR	No action	Protected path forced switch to protection
MANWKSWBK	No action	Manual switch of protected back
MANWKSWPR	No action	Manual switch of protected to protecting
TIMCHG	No action	Trace identification message change
WKSWBK	No action	Protected path switch back
WKSWPR	No action	Protected path switch to protection
WTRREVERT	No action	Wait to revert time-out; reported as switch reason

[1] *Find the BLSR path that failed and correct the problem.*
[2] *Look for and troubleshoot related STS1 alarms.*

Alarm/Condition – AISP, PATHSEL, or PROTNA

14 Perform steps 15 through 25 at each NE in the network. Start with the nearest NE.

15 Retrieve alarms [DLP-100].

16 Are there any equipment alarms?

If yes, resolve alarms per TAP-021.
If no, then continue to step 17.

17 Are there any OCn facility alarms?

If yes, resolve alarms per TAP-029.
If no, then continue to step 18.

18 Are there any EC1 facility alarms?

If yes, resolve alarms per TAP-022.
If no, then continue to step 19.

19 Are there any T3 (DS3) facility alarms?

If yes, resolve alarms per TAP-043.
If no, then continue to step 20.

20 Retrieve cross-connection for STS path [DLP-504] and verify that it is correct.

21 Is the cross-connection for STS path in place?

If yes, go to step 24.
If no, then continue to step 22.

22 Re-establish STS path cross-connect [DLP-504].

23 Does STS path have a parent facility?

NOTE: *An STS path on an LIF901 or LIFG01 unit does not have a parent facility. The STS path is created when an LIF901 or LIFG01 unit is assigned.*

If yes, go to step 24.
If no, then go to step 26.

24 What is service state of parent facility [DLP-501]?

If parent facility is in-service, then go to step 26.
If out-of-service or in maintenance state, then continue to step 25.

25 Place parent facility in-service [DLP-501].

26 Have all NEs been checked?

If yes, then contact Customer Service.
If no, then continue to step 27.

27 Retrieve alarms at next NE in the network [DLP-100]; then return to step 16.

28 STOP. This procedure is complete.

Alarm/Condition – BERP-HT or BERP-LT

29 **CAUTION: Possibility of service interruption. Follow the replacement procedure in DLP-101 for the HIF/LIF to avoid loss of traffic.**

30 Replace the HIF or LIF [DLP-101] that is carrying the alarmed STS path; then retrieve STS alarms/conditions [DLP-100].

31 Did alarm clear (may take several minutes)?

If yes, STOP. This procedure is complete.
If no, then continue to step 32.

32 Problem must be at far-end NE. Analyze alarms at far-end NE per TAP-001.

33 If problem persists, test fiber facility per local procedure or contact Customer Service.

34 STOP. This procedure is complete.

Alarm/Condition – BLSRPATHNA

35 Are there any BLSR ring alarms [DLP-100]?

If yes, go to TAP-058 and clear BLSR ring alarms.
If no, then continue to step 36.

36 Check STS cross-connect between ENTRY nodes and EXIT nodes [DLP-504].

37 Is cross-connection provisioned correctly?

If yes, go to step 40.
If no, then continue to step 38.

38 Re-establish STS path cross-connect [DLP-504]; then retrieve alarms [DLP-100].

39 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 40.

40 Are there any OC48 facility alarms [DLP-100]?

If yes, go to TAP-029 and clear OC48 facility alarms.
If no, then continue to step 41.

41 Are there any equipment alarms [DLP-100]?

If yes, go to TAP-021.
If no, then continue to step 42.

42 Are there any other STS path alarms [DLP-100]?

If yes, return to step 13 and clear other path alarms.
If no, contact Customer Service.

43 STOP. This procedure is complete.

Alarm/Condition – BRIDGE

44 Check each NE on the ring for BLSR ring alarms [DLP-100].

45 Are there any BLSR ring alarms?

If yes, go to TAP-058 and clear BLSR ring alarms.
If no, contact Customer Service.

46 STOP. This procedure is complete.

Alarm/Condition – CONCAT

47 ***NOTE:*** *A CONCAT alarm is only detected in the receive direction and may be caused by another vendor's equipment. In this procedure, references to a far-end/adjacent NE assume the NE is a 1603 SMX, 1603 SM, or 1603 SE. For other vendor's equipment, refer to appropriate documentation.*

Perform steps 48 through 57 at each NE in the network, starting with the local NE.

48 Retrieve alarms [DLP-100].

49 Are there any equipment, facility, or other path alarms?

If yes, then continue to step 50.
If no, then go to step 51.

50 Resolve alarms before proceeding. To clear equipment alarms go to TAP-021; to clear facility alarms go to TAP-029 (OCn), TAP-022 (EC1), or TAP-043 (T3); and to clear other path alarms return to step 13.

51 What is service state of parent facility [DLP-501]?

If out-of-service or in maintenance state, go to step 52.
If in-service, go to step 53.

52 Change service state of parent facility to in-service [DLP-501].

53 What is service state of alarmed path [DLP-501]?

If in-service or memory administration, go to step 55.
If maintenance, then continue to step 54.

54 Change path service state to memory administration [DLP-501].

55 Retrieve cross-connect for STS path and verify that it is correct [DLP-504].

56 Is the cross-connection for STS path in place?

If yes, go to step 58.
If no, then continue to step 57.

57 Re-establish STS path cross-connect [DLP-504].

58 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service.

59 STOP. This procedure is complete.

Alarm/Condition – ETFAIL

60 Retrieve alarms [DLP-100].

61 Are there any BLSR ring alarms?

If yes, go to TAP-058 and clear BLSR ring alarms.
If no, then continue to step 62.

62 Are there any OC48 facility alarms?

If yes, go to TAP-029 and clear OC48 facility alarms.
If no, then continue to step 63.

63 Are there any equipment alarms?

If yes, then go to TAP-021.
If no, contact Customer Service.

64 STOP. This procedure is complete.

Alarm/Condition – FRCD or LOCKOUT

65 **CAUTION: Possibility of service interruption. The FRCD or LOCKOUT condition should not be allowed under normal conditions. This condition prevents the path selector from automatically switching to the protecting path if a failure occurs in the ring network requiring the selector to switch, which would interrupt service.**

66 ***NOTE:*** *If revertive switching is not enabled, the switch can be released and the selected path remains active.*

To clear the alarm, release the forced or locked-out switch [DLP-545].

67 STOP. This procedure is complete.

Alarm/Condition – INHPMREPT

68 To clear the alarm, allow PM reporting on STS path [DLP-510].

69 STOP. This procedure is complete.

Alarm/Condition – LOMF

70 Retrieve STS alarms [DLP-100].

71 Is there an AISP alarm?

If yes, then go to step 14.
If no, then continue to step 72.

72 At the far-end NE that terminates the STS path, determine STS1 payload type [DLP-511].

73 Is Payload Type = VT?

If yes, go to step 76.
If no, then continue to step 74.

74 Change STS1 path payload type to VT [DLP-511]; then retrieve alarms [DLP-100].

75 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 76.

76 Look for other alarms per TAP-001. If alarm cannot be isolated, contact Customer Service.

77 STOP. This procedure is complete.

Alarm/Condition – LOP (STS1 - Rcv Direction)

78 Log on to the NE with the alarm [DLP-117]; then retrieve alarms [DLP-100].

79 Are there any equipment, facility, or other path alarms?

If yes, then continue to step 80.
If no, then go to step 81.

80 Resolve these alarms before proceeding. To clear equipment alarms go to TAP-021; to clear facility alarms go to TAP-029 (OCn), TAP-022 (EC1), or TAP-043 (T3); and to clear other path alarms return to step 13.

81 Determine payload type [DLP-511].

82 Is payload type correct (i.e., VT or STS)?

If yes, go to step 85.
If no, then continue to step 83.

83 Change payload type to VT or STS [DLP-511]; then retrieve alarms [DLP-100].

84 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 85.

85 Has the payload type been checked for all NEs in the path?

If yes, contact Customer Service.
If no, then continue to step 86.

86 Log on to the next NE in the path [DLP-117].

87 Retrieve alarms [DLP-100]; then return to step 79.

88 STOP. This procedure is complete.

STS1 – LOP (STS1 - Trmt Direction)

89 Retrieve alarms at the local NE and check for equipment alarms [DLP-100].

90 Are there any equipment alarms?

If yes, go to TAP-021.
If no, then continue to step 91.

91 Are there any DS3 or USRLAN facility alarms [DLP-100]?

If yes, go to TAP-043 to clear DS3 alarms or TAP-057 to clear USRLAN alarms.
If no, then continue to step 92.

92 Are there any other STS1 path alarms besides LOP (trmt) [DLP-100]?

If yes, return to step 13 and clear other STS1 path alarms.
If no, contact Customer Service.

93 STOP. This procedure is complete.

Alarm/Condition – LOP (STS3c/STS12c)

94 ***NOTE:*** *An LOP alarm on an STS3c or STS12c path is detected in the receive direction for OCn facility, and in the receive and transmit direction for USRLAN STS path (LIF901/G01). The far-end/adjacent NE equipment where the alarm originates may be another vendor's equipment. Any references to a far-end/adjacent NE in this procedure apply to a 1603 SMX, 1603 SM, or 1603 SE. For other vendor's equipment, refer to appropriate documentation.*

Log on to the NE with the alarm [DLP-117]; then retrieve alarms [DLP-100].

95 Are there any equipment, facility, or other path alarms?

If yes, then continue to step 96.
If no, then go to step 98.

96 Resolve these alarms before proceeding. To clear equipment alarms go to TAP-021; to clear facility alarms go to TAP-029 (OCn), TAP-022 (EC1), or TAP-043 (T3); and to clear other STS path alarms return to step 13.

97 Does STS path have a parent facility?

NOTE: *An STS path on an LIF901 or LIFG01 unit does not have a parent facility. The STS path is created when an LIF901 or LIFG01 unit is assigned.*

If yes, go to step 98.
If no, then go to step 100.

98 What is service state of parent facility [DLP-501]?

NOTE: *There is no parent facility for STS3c on an LIF901 unit. On an LIF901, the STS3c path is created when LIF901 EQPT is assigned.*

NOTE: *There is no parent facility for STS12c on an LIFG01 unit. On an LIFG01, the STS12c path is created when LIFG01 EQPT is assigned.*

If parent facility is in-service, go to step 100.
If out-of-service or in maintenance state, then go to step 99.

99 Change service state of facility to in-service [DLP-501].

100 What is service state of alarmed path [DLP-501]?

If in-service or memory administration, go to step 102.
If out-of-service, then continue to step 101.

101 Change service state of alarmed path to memory administration [DLP-501].

102 Retrieve cross-connect for STS path and verify that it is correct [DLP-504].

103 Is the cross-connection for STS path in place?

If yes, go to step 105.
If no, then continue to step 104.

104 Re-establish STS path cross-connect [DLP-504]; then retrieve alarms [DLP-100].

105 Did LOP alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 106.

106 Have all NEs in the path been checked?

If yes, contact Customer Service.
If no, then go to step 107.

107 Log on to the next NE in the path [DLP-117].

108 Retrieve alarms [DLP-100]; then return to step 95.

109 STOP. This procedure is complete.

Alarm/ Condition – MAN

110 ***NOTE:*** *The MAN condition is the lowest priority level and does not affect service if left in this state; however, the alarm remains active. If revertive switching is not enabled, the switch can be released and the selected path remains active.*

To clear the alarm, release protection switching [DLP-507].

111 STOP. This procedure is complete.

Alarm/Condition – PDI (STS1 - Rcv Direction)

112 Retrieve alarms and conditions for the upstream NE [DLP-100] where the payload was mapped into the STS Synchronous Payload Envelope (SPE) (i.e., at the path origin).

113 What is the payload type?

If VT, go to step 114.
If DS3, go to step 115.
If something other than VT or DS3, then go to step 116.

114 Is there an AIS or LOP alarm on one or more VT paths?

If yes, go to TAP-038.
If no, then go to step 116.

115 Is there an AIS, LOS, or OOF alarm on the DS3 path?

If yes, go to TAP-043.
If no, then continue to step 116.

116 ***NOTE:*** *A PDI value has been inserted in the C2 byte because of one or more failures at the upstream NE.*

If the cause cannot be corrected, disable PDI at the local NE by changing the signal label to 1 (i.e., equipped – nonspecific payload) [DLP-509].

117 If problem persists, contact Customer Service.

118 STOP. This procedure is complete.

Alarm/Condition – PDI (STS1 - Trmt Direction)

119 Retrieve alarms at the local NE [DLP-100].

120 Are there any equipment alarms?

If yes, go to TAP-021.
If no, then continue to step 121.

121 Are there any DS3 facility alarms?

If yes, go to TAP-043.
If no, then continue to step 122.

122 Are there any STS1 path alarms besides PDI?

If yes, then return to step 13 and clear other STS1 path alarms.
If no, contact Customer Service.

123 STOP. This procedure is complete.

Alarm/Condition – PDI (STS3c/STS12c)

124 ***NOTE:*** *A PDI value has been inserted in the C2 byte because of one or more failures at the upstream NE.*

If the cause cannot be corrected, disable PDI at the local NE by changing the signal label to 1 (i.e., equipped – nonspecific payload) [DLP-509].

125 If problem persists, contact Customer Service.

126 STOP. This procedure is complete.

Alarm/Condition – PLM (STS1 - Rcv Direction)

127 ***NOTE:*** *For hardware units that do not support PDI detection, a PLM alarm may be raised when PDI values are present in the C2 byte.*

See Figure 1 for STS1 signal label monitoring points in the 1603 SMX NE.

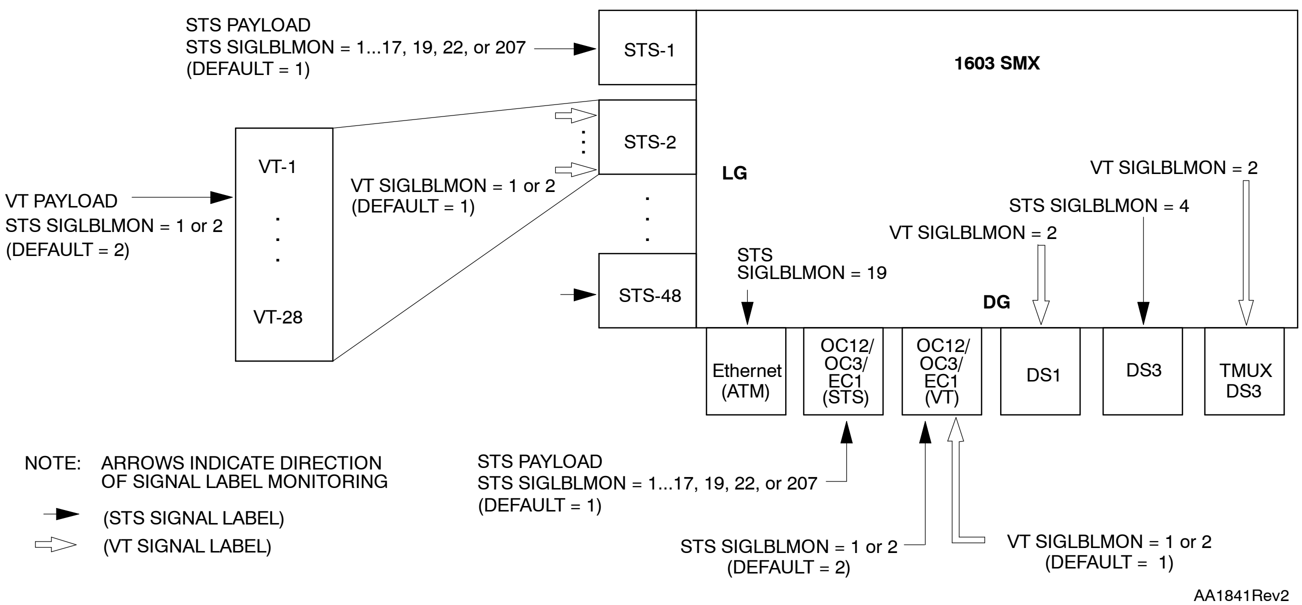


Figure 1. Signal Label Monitoring – STS1 (C2 Byte) and VT (V5 Byte)

128 Retrieve STS1 conditions [DLP-100].

129 To determine the incoming signal label, which is in the C2 byte, locate SIGLBL-xx in the Condition column on the Alarms work view.

130 Note the number following SIGLBL; then find that number in Table B to identify the contents of the STS Synchronous Payload Envelope (SPE).

Table B. STS1 Path Signal Label Assignments *

Byte C2 Code Decimal (Hex)	Contents of the STS1 SPE
0 (00)	Unequipped
1 (01)	Equipped — nonspecific payload
2 (02)	Floating VT mode (EC1 and OCn STS1 paths provisioned for VT payload)
3 (03)	Locked VT mode
4 (04)	Asynchronous mapping for DS3 (T3 port)
19 (13)	Mapping for ATM
22 (16)	HDLC-over-SONET mapping (PPP scrambling is on)
207 (CF)	HDLC-over-SONET mapping (PPP scrambling is off)

* *From BellCore Document GR-253-CORE, Issue 2, Dec. 1995. Note that values not listed are not defined for STS1 or are used to indicate Payload Defect Indication (PDI).*

131 Retrieve the expected (provisioned) STS1 signal label [DLP-509].

132 Compare the incoming signal label in the C2 byte and the expected signal label. Determine which is correct. Refer to Table C for recommended corrective actions.

133 STOP. This procedure is complete.

Table C. Clearing STS1 Payload Label Mismatch (PLM) Alarm

LOCATION OF PLM ALARM	PROBABLE CAUSES	RECOMMENDED ACTIONS
Unterminated Line or Drop Group (Payload type=STS1) Allowed values of provisioned STS1 Signal label = 1...17, 19, 22, or 207	Payload type indication in incoming C2 byte is incorrect	Check network cross-connections and change if necessary [DLP-504]. Check payload type at path origin and change if necessary [DLP-511].
	Expected STS1 Signal Label parameter is incorrectly provisioned	Change provisioned value of expected STS1 signal label parameter to agree with the signal label in C2 byte [DLP-509].
	Payload Defect Indication (PDI) in incoming C2 byte	Resolve network problem, or disable PDI at path origin (*recommended*), or silence alarm by provisioning STS1 signal label to (1) Equipped - nonspecific payload [DLP-509].
Terminated Line or Drop Group – EC1 or OCn (Payload type=VT) Allowed values of provisioned STS1 Signal label = 1 or 2 [1]	Payload type indication in incoming C2 byte is incorrect	Check network or facility cross-connections and change if necessary [DLP-504]. Check payload type at path or facility origin and change if necessary [DLP-511].
	Payload Defect Indication (PDI) in incoming C2 byte	Resolve facility problem, or disable PDI at path origin (*recommended*), or silence alarm by provisioning STS1 signal label to (1) Equipped - nonspecific payload [DLP-509].
Terminated Drop Group – DS3 (Payload type=STS) STS1 Signal label = 4 (not provisionable) [2]	Payload type indication in incoming C2 byte is incorrect	Check network cross-connections and change if necessary [DLP-504]. Check payload type at facility origin and change if necessary [DLP-511].
	Payload Defect Indication (PDI) in incoming C2 byte	Resolve network problem, or disable PDI at path origin (*recommended*).
Drop Group – Terminated Ethernet (LIF901) (Payload type= ATM) STS Signal Label = 19 (Not provisionable) [3]	Payload type indication in incoming C2 byte is incorrect	Check network cross-connections and change if necessary [DLP-504]. Check payload type at path origin and change if necessary [DLP-511].

[1] *AIS is inserted on VT paths.*

[2] *AIS is inserted on STS payload.*

[3] *AIS is inserted on ATM payload.*

Alarm/Condition – PLM (STS1 - Trmt Direction)

134 Retrieve alarms at the local NE [DLP-100].

135 Are there any equipment alarms?

If yes, go to TAP-021.
If no, then continue to step 136.

136 Are there any DS3 facility alarms?

If yes, go to TAP-043.
If no, then continue to step 137.

137 Are there any other STS1 path alarms?

If yes, then return to step 13 and clear other STS1 path alarms.
If no, contact Customer Service.

138 STOP. This procedure is complete.

Alarm/Condition – PLM (STS3c)

139 See Figure 2 for STS3c signal label monitoring points in the 1603 SMX NE.

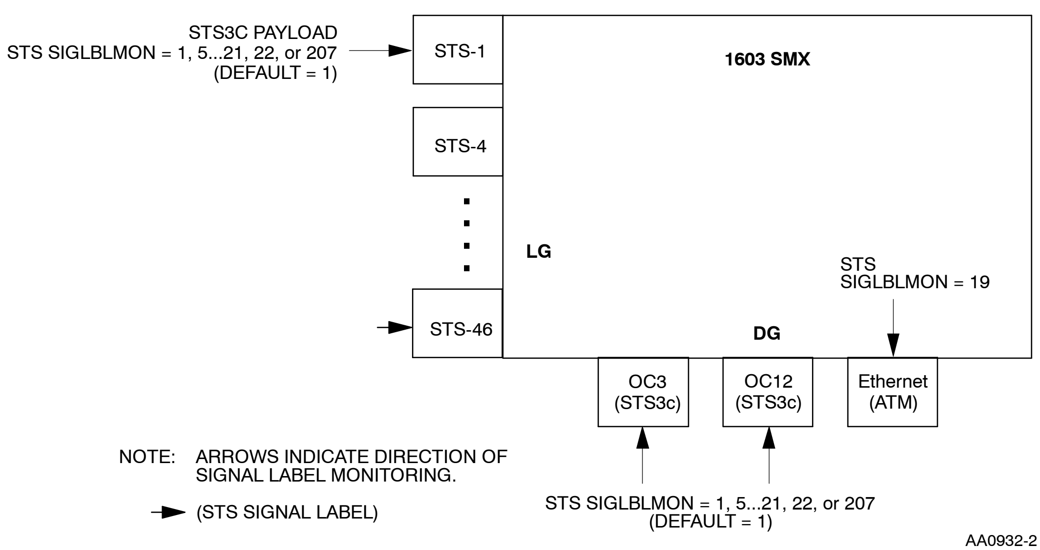


Figure 2. Signal Label Monitoring – STS3c (C2 Byte)

140 Retrieve STS3c conditions [DLP-100].

141 To determine the incoming signal label, which is in the C2 byte, locate SIGLBL-xx in the Condition column on the Alarms work view.

142 Note the number following SIGLBL; then find that number in Table D to identify the contents of the STS Synchronous Payload Envelope (SPE).

Table D. STS3c Path Signal Label Assignments *

BYTE C2 CODE DECIMAL (Hex)	CONTENTS OF THE STS3c SPE
0 (00)	Unequipped
1 (01)	Equipped – nonspecific payload
5 (05)	Mapping for byte observable SYNTRAN
18 (12)	Asynchronous mapping for DS4NA
19 (13)	Mapping for ATM
20 (14)	Mapping for DQDB
21 (15)	Asynchronous mapping for FDDI
22 (16)	Mapping for HDLC over SONET (PPP scrambling is on)
207 (CF)	Mapping for HDLC over SONET (PPP scrambling is off)
* *From BellCore Document GR-253-CORE, Issue 2, Dec. 1995. Note that values not listed are not defined for STS3c or are used to indicate Payload Defect Indication (PDI).*	

143 Determine the expected (provisioned) STS3c signal label [DLP-509].

144 Compare the incoming signal label in the C2 byte and the expected signal label. Determine which is correct. Refer to Table E for corrective actions to take.

145 STOP. This procedure is complete.

146 See Figure 3 for STS12c signal label monitoring points in the 1603 SMX NE.

Table E. Clearing STS3c Payload Label Mismatch (PLM) Alarm

LOCATION OF PLM ALARM	PROBABLE CAUSES	RECOMMENDED ACTIONS
Unterminated Line Group or Drop Group (Payload type = STS3c) Allowed values of provisioned STS3c Signal label = 1, 5...21, 22, or 207	Payload type indication in incoming C2 byte is incorrect	Check network cross-connections and change if necessary [DLP-504]. Check payload type at path origin and change if necessary [DLP-511].
	Expected STS3c Signal Label parameter is incorrectly provisioned	Change STS3c expected signal label to match the signal label in the C2 byte [DLP-509].
	Payload Defect Indication (PDI) in incoming C2 byte	Resolve network problem, or Disable PDI at path origin (*recommended*), or Silence alarm by changing STS3c expected signal label to (1) Equipped - nonspecific payload [DLP-509].
Drop Group — Terminated Ethernet (LIF901) (Payload type = ATM) STS3c Signal label = 19 (Not provisionable)*	Payload type indication in incoming C2 byte is incorrect	Check network cross-connections and change if necessary [DLP-504]. Check payload type at path origin and change if necessary [DLP-511].

* *AIS is inserted on ATM payload.*

Alarm/Condition – PLM (STS12c)

147 Retrieve STS12c conditions [DLP-100].

148 To determine the incoming signal label, which is in the C2 byte, locate SIGLBL-xx in the Condition column on the Alarms work view.

149 Note the number following SIGLBL; then find this number in Table F to identify the contents of the STS Synchronous Payload Envelope (SPE).

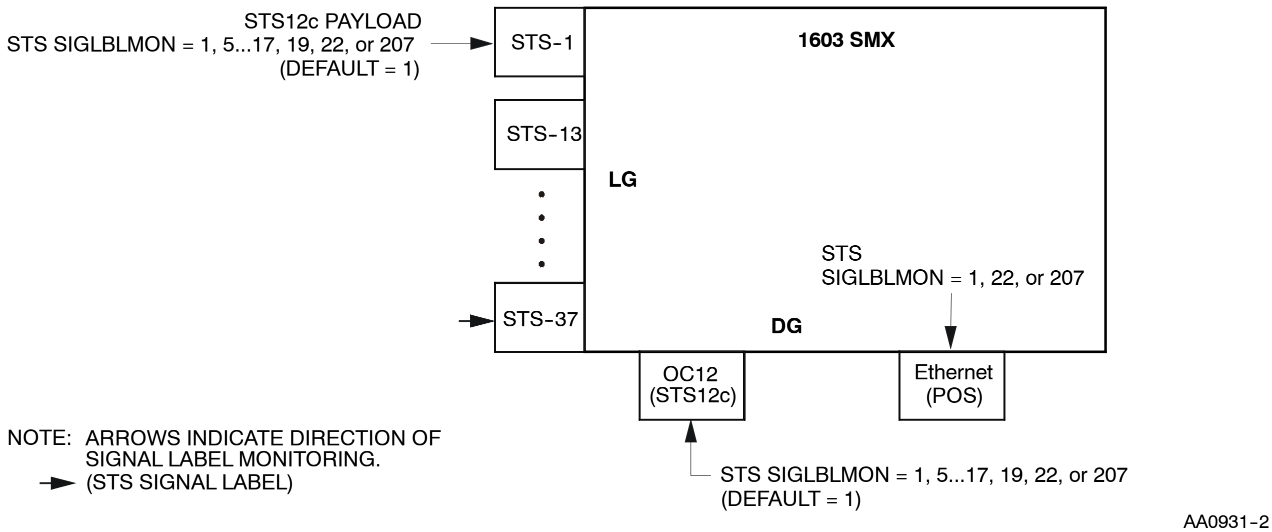


Figure 3. Signal Label Monitoring – STS12c (C2 Byte)

Table F. STS12c Path Signal Label Assignments *

BYTE C2 CODE DECIMAL (HEX)	CONTENTS OF STS12c SPE
0 (00)	Unequipped
1 (01)	Equipped – nonspecific payload
5 (05)	Mapping for byte observable SYNTRAN
19 (13)	Mapping for ATM
22 (16)	Mapping for HDLC over SONET (PPP scrambling is on)
207 (CF)	Mapping for HDLC over SONET (PPP scrambling is off)

* *From BellCore Document GR-253-CORE, Issue 2, Dec. 1995. Note that values not listed are not defined for STS12c or are used to indicate Payload Defect Indication (PDI).*

150 Determine the expected (provisioned) STS12c signal label [DLP-509].

151 Compare the incoming signal label in the C2 byte and the expected signal label. Determine which is correct. Refer to Table G for corrective actions to take.

152 STOP. This procedure is complete.

Table G. Clearing STS12c Payload Label Mismatch (PLM) Alarm

LOCATION OF PLM ALARM	PROBABLE CAUSES	RECOMMENDED ACTION
Line Group or Drop Group— Unterminated (Payload type = STS12c) Allowed values of provisioned STS12c Signal label = 1, 5...17, 19, 22, or 207	Payload type indication in incoming C2 byte is incorrect	Check network cross-connections and change if necessary [DLP-504]. Check payload type at path origin and change if necessary [DLP-511].
	Expected STS12c Signal Label parameter is incorrectly provisioned	Change STS12c expected signal label to match the signal label in the C2 byte [DLP-509]
	Payload Defect Indication (PDI) in incoming C2 byte	Resolve network problem, or Disable PDI at path origin (*recommended*), or Silence alarm by changing STS12c expected signal label to (1) Equipped - nonspecific payload [DLP-509].
Drop Group — Terminated Ethernet (LIFG01) (Payload type = STS12c) Allowable values of STS12c Signal label = 1, 22, 207	Payload type indication in incoming C2 byte is incorrect	Check network cross—connections and change if necessary [DLP—504]. Check payload type at path origin (recommended) and change if necessary [DLP—511]. Silence alarm by changing STS12c expected signal label to (1) Equipped — nonspecific payload [DLP—509].

Alarm/Condition – RFI

153 ***NOTE:*** *A failure has been detected along the downstream STS path. Probable cause is equipment or facility problems at local NE or between local NE and far-end NE that terminates this path.*

See Figure 4 for an example network.

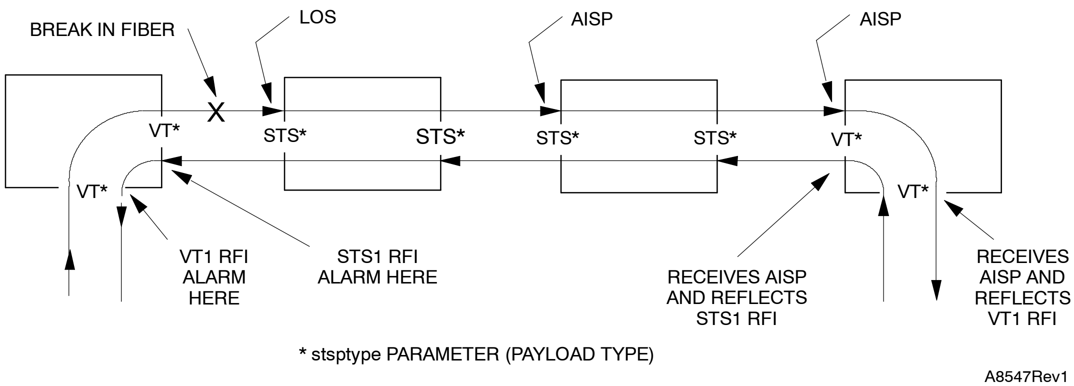


Figure 4. Example Network

154 Look for other alarms that would cause the RFI alarm. Refer to TAP-001.

155 STOP. This procedure is complete.

Alarm/Condition – RFIMM

156 Check the provisioning of the Enhanced Remote Defect Indicator (ERDI) parameter at the near-end NE and at the far-end NE [DLP-516].

157 Is the ERDI parameter provisioned the same at both ends of the STS path?

If yes, contact Customer Service.
If no, then continue to step 158.

158 Change the ERDI parameter at either the near-end or far-end NE so the modes agree [DLP-516].

159 STOP. This procedure is complete.

Alarm/Condition – SQUELCH

160 Go to TAP-058 and resolve BLSR failures around the ring.

161 STOP. This procedure is complete.

Alarm/Condition –TIM

162 Determine Provisioned Incoming path trace and Received Incoming path trace [DLP-512].

163 Is Provisioned Incoming or Received Incoming path trace value in error?

If Provisioned Incoming, then continue to step 164.
If Received Incoming, then go to step 166.

164 Change the STS Provisioned Incoming path trace to match the Received Incoming path trace [DLP-512].

165 STOP. This procedure is complete.

166 Log on at the far-end NE that is supposed to terminate this STS path [DLP-117].

167 Determine Provisioned Outgoing path trace [DLP-514].

168 From response, is Provisioned Outgoing message as expected (should be the same as the Provisioned Incoming value at the NE with the TIM alarm)?

If yes, go to step 171.
If no, then continue to step 169.

169 Change the Provisioned Outgoing message [DLP-514].

170 STOP. This procedure is complete.

171 ***NOTE:*** *STS traffic (payload) is not being delivered between the intended NEs.*

Interrogate intermediate NEs to determine where STS payload is misdirected.

172 Starting with NE nearest originating NE, log on [DLP-117]; then retrieve cross-connections [DLP-504].

173 Is cross-connect correct?

If yes, then continue to step 174.
If no, then go to step 175.

174 Have cross-connects been checked on all NEs in STS path?

If yes, contact Customer Service.
If no, return to step 172 and retrieve cross-connections at next NE in STS1 path.

175 Re-establish STS path cross-connect [DLP-504]; then retrieve alarms at NE with TIM alarm [DLP-100].

176 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 177.

177 Have cross-connects been checked for all NEs in the STS path?

If yes, then contact Customer Service.
If no, then return to step 172 and retrieve cross-connections at next NE in STS path.

178 STOP. This procedure is complete.

Alarm/Condition – T-xxx

179 ***NOTE:*** *A threshold crossing alert (TCA) is generated when a performance parameter exceeds the value specified for it. As a default, a TCA is reported as an event. However, if the Notification Code attribute is changed to minor (MN), major (MJ), or critical (CR), a TCA is reported as an alarm.*

Refer to Table H for STS PM thresholds.

180 **CAUTION: Possibility of service interruption. Follow the replacement procedure in DLP-101 when replacing a plug-in unit to avoid loss of traffic.**

181 Is the condition severe enough to warrant unit replacement?

If yes, go to step 183.
If no, record the alarm as an event.

182 STOP. This procedure is complete.

Table H. STS PM Thresholds

MONITOR TYPE	PATH	FACTORY DEFAULT		RANGE	DESCRIPTION
		15-MIN	1-DAY		
BERP-HT	STS1	4		3...4	Bit Error Ratio Path – High threshold (SFBER)
BERP-HT	STS3c			4	
	STS12c			4	
BERP-LT	All STS paths	6		5...9	Bit Error Ratio Path – Low threshold (DGBER)
CVP	STS1	15	125	1...4,294,967,295	Coding violation count – path (near end or far end)
	STS3c	25	250	1...4,294,967,295	
	STS12c	75	750	1...4,294,967,295	
DSESP	STS1	2400		1...65535	Number of coding violations to make one SESP (one threshold used by both near end or far end counts)
	STS3c	2400		1...65535	
	STS12c	8600		1...65535	
ESP	STS1	12	100	1...65535	STS Path Errored Seconds (near end or far end)
	STS3c	20	200	1...65535	
	STS12c	60	600	1...65535	
NPJCDET	All STS paths	60	5760	1...4,294,967,295	Negative Pointer Justification Count Detected
NPJCGEN	All STS paths	60	5760	1...4,294,967,295	Negative Pointer Justification Count Generated
PPJCDET	All STS paths	60	5760	1...4,294,967,295	Positive Pointer Justification Count Detected
PPJCGEN	All STS paths	60	5760	1...4,294,967,295	Positive Pointer Justification Count Generated
PJCSDET	All STS paths	60	5760	1...65535	Positive Justification Count Seconds Detected
PJCSGEN	All STS paths	60	5760	1...65535	Positive Justification Count Seconds Generated
PJCDIFF	All STS paths	60	5760	1...4,294,967,295	Pointer Justification Count Difference

Table H. STS PM Thresholds

MONITOR TYPE	PATH	15-MIN	1-DAY	RANGE	DESCRIPTION
SESP	All STS paths	3	7	1...65535	STS Path Severely Errored Seconds (near end or far end)
UASP	All STS paths	10	10	1...65535	STS Path Unavailable Seconds (near end or far end)

183 Retrieve alarms at the local and far-end NE [DLP-100].

184 Are there any CCM, CLK, or SYNCN alarms?

If CLK or CCM, go to TAP-021.
If SYNCN, go to TAP-027.
If no, then continue to step 185.

185 Is the HIF or LIF carrying the alarmed path generating a SYNCCLK alarm?

If yes, go to TAP-021.
If no, then continue to step 186.

186 What type of facility is carrying the alarmed STS path?

If OC3, OC12, or OC48, continue to step 187.
If DS3, go to step 192.
If EC1, then go to step 194.

187 Replace the HIF or LIF [DLP-101] carrying the alarmed STS path, wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The 1301 NMX retrieves register values specified by the number of seconds shown in the Refresh Rate field.*

188 Did PM errors stop?

If yes, STOP. This procedure is complete.
If no, then continue to step 189.

189 Problem must be at far-end terminal. Analyze alarms per TAP-001 at far-end NE.

190 If problem persists, test fiber facility per local procedure or contact Customer Service.

191 STOP. This procedure is complete.

192 Check for CCM unit alarms [TAP-021]; then check upstream path for other failures.

193 Was problem found and cleared?

If yes, STOP. This procedure is complete.
If no, then continue to step 194.

194 ***NOTE:*** *The far end is detecting a problem on the receive (facility) side. Problem is most likely at near-end equipment or on the facility.*

Refer to Table I and locate the type of LIF associated with the facility that is carrying the alarmed STS path. Go to the step referenced in the table to clear the alarm.

Table I. Types of LIFs

IF DROP GROUP IS EQUIPPED WITH AN...	AND UNIT IS...	THEN GO TO...
LIF201/LIF301	Non-redundant	Step 195
	Redundant	Step 209
LIF501/LIF701	Non-redundant	Step 195
	Redundant	Step 227
LIFD01	Non-redundant	Step 235
	Redundant	Step 248

Non-Redundant LIF201/LIF301/LIF501/LIF701 Unit

195 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF and LDR units. If facility is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

196 At the near-end NE, place LIF carrying alarmed STS path in maintenance state [DLP-501].

197 Run all diagnostic phases on this LIF [DLP-500]. Perform one iteration.

198 Did diagnostics pass?

If yes, go to step 200.
If no, then replace LIF per DLP-101.

199 STOP. This procedure is complete.

200 Place LIF back in-service [DLP-501].

201 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR.**

202 Place LDR associated with LIF in maintenance state [DLP-501].

203 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

204 Did diagnostics pass?

If yes, go to step 206.
If no, then replace LDR per DLP-101.

205 STOP. This procedure is complete.

206 Place LDR back in-service [DLP-501].

207 Problem most likely in facility that is carrying the alarmed STS1 path. Troubleshoot per local practice.

208 STOP. This procedure is complete.

Redundant LIF201/LIF301 Unit

The active and standby LIFs associated with the facility carrying the alarmed STS path will be switched to determine whether the active LIF or active LDR is causing the alarm.

209 Switch the active LIF carrying the alarmed STS path to standby [DLP-505].

NOTE: *When LIF20x/30x units are switched, the LDRs also switch (i.e., LDR-A is active when LIF-A is active, and LDR-B is active when LIF-B is active).*

210 Wait several minutes; then retrieve PM registers for the path [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

211 Did PM errors stop?

If yes, go to step 214.
If no, then continue to step 212.

212 Problem most likely in facility. Troubleshoot per local practice.

213 STOP. This procedure is complete.

214 Problem must be in either the LIF or LDR that are now in standby. Continue to step 215 and perform diagnostics on LIF.

215 **CAUTION: Possibility of service interruption. Diagnostics are service-affecting if performed on active units. Be sure the LIF and LDR units are in maintenance state before performing diagnostics.**

216 Place LIF that is in standby in maintenance state [DLP-501].

217 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

218 Did diagnostics pass?

If yes, go to step 220.
If no, replace LIF per DLP-101.

219 STOP. This procedure is complete.

220 Place LDR to be tested in maintenance state [DLP-501].

221 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

222 Did diagnostics pass?

If yes, go to step 224.
If no, replace LDR per DLP-101.

223 STOP. This procedure is complete.

224 Place LIF and LDR back in-service [DLP-501]; then go to step 225.

225 Problem most likely in facility that is carrying the alarmed STS1 path. Troubleshoot per local practice.

226 STOP. This procedure is complete.

Redundant LIF501/LIF701 Unit

NOTE: *The active and standby LIFs associated with the facility carrying the alarmed STS1 path will be switched to determine whether the active LIF is causing the alarm. If the alarm isn't cleared, the active and standby LDRs associated with the alarmed LIF will be switched.*

227 Switch active LIF carrying the alarmed STS1 path to standby [DLP-505].

228 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

229 Did PM errors stop?

If yes, replace LIF that is now in standby per DLP-101.
If no, go to step 231.

230 STOP. This procedure is complete.

231 Switch the active LDR carrying the alarmed STS1 path to standby [DLP-505].

232 Wait several minutes; then retrieve PM registers [DLP-517].

233 Did PM errors stop?

If yes, replace standby LDR per DLP-101.
If no, problem is most likely in facility. Troubleshoot per local practice.

234 STOP. This procedure is complete.

Non-Redundant LIFD01 Unit

235 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF unit. If EC1 facility is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

236 Place LIF carrying alarmed STS path in maintenance state [DLP-501].

237 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

238 Did diagnostics pass?

If yes, go to step 240.
If no, replace LIF per DLP-101.

239 STOP. This procedure is complete.

240 Place LIF back in-service [DLP-501].

241 Identify the LDR that is carrying the alarmed STS1 path [DLP-565] and switch that LDR to protection [DLP-529].

NOTE: *Revertive switch may occur. Inhibit switch back to working if required.*

242 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

243 Did PM errors stop?

If yes, replace LDR that was switched to protection [DLP-101].
If no, then go to step 245.

244 STOP. This procedure is complete.

245 If switch back to working was inhibited, allow automatic switching to working unit [DLP-506].

246 Problem most likely in facility carrying the alarmed STS1 path. Troubleshoot per local practice.

247 STOP. This procedure is complete.

Redundant LIFD01 Unit

NOTE: *The active and standby LIFs associated with the alarmed facility will be switched to determine whether the active LIF is causing the alarm. If the alarm isn't cleared, the protection LDR and the LDR associated with the alarmed facility will be switched.*

248 Switch the active LIF carrying the alarmed STS1 path to standby [DLP-505].

249 Wait several minutes; then retrieve PM registers [DLP-117].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

250 Did PM errors stop?

If yes, replace LIF that is now in standby [DLP-101].
If no, then go to step 252.

251 STOP. This procedure is complete.

252 Identify the LDR that is carrying the alarmed STS1 path [DLP-565] and switch that LDR to protection [DLP-529].

NOTE: *Revertive switch may occur. Inhibit switch back to working if required.*

253 Wait several minutes; then retrieve PM registers [DLP-517].

254 Did PM errors stop?

If yes, go to step 255.
If no, then go to step 257.

255 Identify the physical location of the LDR that was switched to protection [DLP-565] and replace that LDR per DLP-101.

256 STOP. This procedure is complete.

257 If switch back to working was inhibited, allow automatic switching to working unit [DLP-506].

258 Problem most likely in facility that is carrying the alarmed STS path. Troubleshoot per local practice.

259 STOP. This procedure is complete.

Alarm/Condition – UNEQ

260 Check STS cross-connects at each upstream NE starting with nearest originating NE.

261 Retrieve cross-connections at nearest originating NE [DLP-504].

262 Is cross-connection correct?

If yes, then continue to step 263.
If no, then go to step 264.

263 Have cross-connects been checked on all upstream NEs?

If yes, contact Customer Service.
If no, return to step 261 and retrieve cross-connections at next upstream NE.

264 Re-establish STS path cross-connect [DLP-504]; then retrieve alarms at NE with UNEQ alarm [DLP-100].

265 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, then continue to step 266.

266 Have cross-connects been checked on all upstream NEs?

If yes, contact Customer Service.
If no, return to step 261 and retrieve cross-connections at next upstream NE.

267 STOP. This procedure is complete.

TAP-035
Clear DS1 Facility Alarm (External T1 Facility on DMIxxx)

Purpose

Provides procedures for clearing DS1 facility alarms.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Retrieve alarms [DLP-100].
2	Are there any DMI or VTG alarm indications on drop group with alarmed DS1? If yes, refer to TAP-021 to clear alarm. If no, go to step 3.
3	Have DS1 alarms and conditions been retrieved? If yes, go to step 5. If no, go to step 4.
4	Retrieve DS1 alarms and conditions [DLP-100].
5	Identify the alarm condition(s) and Access Identifier (refer to Table A); then go to the step indicated in Table B to clear alarm.

Table A. DS1 (T1)-to-VT1 Assignment (Sequential and Grouped AID Formats*)

	VTG 1				VTG 2				VTG 3				VTG 4				VTG 5				VTG 6				VTG 7			
T1 SEQ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
VT1.5 SEQ	1	8	15	22	2	9	16	23	3	10	17	24	4	11	18	25	5	12	19	26	6	13	20	27	7	14	21	28
VT1.5 and T1 grp	1-1	1-2	1-3	1-4	2-1	2-2	2-3	2-4	3-1	3-2	3-3	3-4	4-1	4-2	4-3	4-4	5-1	5-2	5-3	5-4	6-1	6-2	6-3	6-4	7-1	7-2	7-3	7-4

* *The AID format used is determined by the setting of the VT1/DS1 Numbering Format parameter (System>General>Global Settings).*

Table B. DS1 Facility Alarms/Conditions/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
AIS	Alarm Indication Signal, all ones (NEND RCV)	6
	Alarm Indication Signal, all ones (NEND TRMT)	6
BERL-HT	Line Bit Error Ratio - High Threshold. Line bit error ratio has exceeded a pre-set high threshold setting.	12
DS1ISD	DS1 Idle Signal Detected (NEND RCV). A normal signal source is not present. The far end is probably transmitting an idle signal because of an unassigned DS1 of a DSC. This alarm only applies to SF and ESF formats.	23
INHLPBK-( )	Inhibit loopback (ESFLINE, INBANDRX, or INBANDTX)	26
INHPMREPT	Inhibit Performance Monitoring Reporting. Autonomous reporting of performance monitoring data has been inhibited on DS1 facility.	28
LOF	Loss-of-Frame (NEND RCV). An out-of-frame condition has persisted for more than 3 ms plus alarm delay time. The LOF is detected in the mux direction from the DS1 facility.	54
	Loss-of-Frame (NEND TRMT). The LOF is detected in the demux direction from the SONET network. Problem could be: end-to-end mismatch of T1 provisioning; LOF on far-end facility; equalization at remote LTE; VTG failure on either end; or network problems (incorrect cross-connect, etc.).	54
LOS	Loss-of-Signal (NEND RCV/TRMT). An all zeros pattern exists on the DS1 incoming signal at the DS1 facility.	30
MTCE	Removed from service for maintenance	91
RAI	Remote Alarm Indication (NEND RCV/TRMT). Failures at the far end result in the transmission of a continuous RAI signal in the reverse direction (i.e., toward the near-end NE). These failures include: equipment failure that is DS1 service-affecting, LOS, LOF and AIS. RAI, which replaces the yellow alarm, is only applicable to SF and ESF formats.	93
T-BPV	Bipolar violation — TCA* (NEND RCV)	99
T-CSSP	Controlled slip seconds — Path TCA* (FEND RCV)	99
	Controlled slip seconds — Path TCA* (FEND TRMT)	99
T-CVL	Coding violations — Line TCA* (NEND RCV)	99
T-CVP	Coding violations — Path TCA* (NEND RCV)	99
	Coding violations — Path TCA* (NEND TRMT)	99
	Coding violations — Path TCA* (FEND RCV)	99
	Coding violations — Path TCA* (FEND TRMT)	99

Table B. DS1 Facility Alarms/Conditions/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
T-ESL	Error seconds – Line TCA* (NEND RCV)	99
	Error seconds – Line TCA* (FEND RCV)	99
	Error seconds – Line TCA* (FEND TRMT)	99
T-ESP	Error seconds – Path TCA* (NEND RCV)	99
	Error seconds – Path TCA* (NEND TRMT)	99
	Error seconds – Path TCA* (FEND RCV)	99
	Error seconds – Path TCA* (FEND TRMT)	99
T-SASP	SEF/AIS seconds – Path TCA* (NEND RCV)	99
	SEF/AIS seconds – Path TCA* (NEND TRMT)	99
T-SEFS	Severely errored framing seconds TCA* (FEND RCV)	99
	Severely errored framing seconds TCA* (FEND TRMT)	99
T-SESL	Severely errored seconds – Line TCA* (NEND RCV)	99
T-SESP	Severely errored seconds – Path TCA* (NEND RCV)	99
	Severely errored seconds – Path TCA* (NEND TRMT)	99
	Severely errored seconds – Path TCA* (FEND RCV)	99
	Severely errored seconds – Path TCA* (FEND TRMT)	99
T-UASP	Unavailable seconds – Path TCA* (NEND RCV)	99
	Unavailable seconds – Path TCA* (NEND TRMT)	99
	Unavailable seconds – Path TCA* (FEND RCV)	99
	Unavailable seconds – Path TCA* (FEND TRMT)	99
Condition	**Description**	**Action**
ACTLPBK	Loopback is active (Loopback type, location, request types are displayed as comment)	No Action
AINS	Automatic-In-Service state	No Action
CONNTESTACT	Test T1 is connected (Pattern = IDLE or QRSS are displayed as comment)	No Action
TSA-n	Test access mode; where: n = MONE, MONF, SPLTA, SPLTB, SPLTE, SPLTF, LOOPE, or LOOPF	No Action
TSN-n	Test access session number assigned to DS1 under test, where: n = 1...999	No Action
QRSS	Quasi-random pattern is detected on RCV facility	No Action

Table B. DS1 Facility Alarms/Conditions/Events (cont)

Event	Description	Action
ACTLPBK	Loopback is activated	No Action
AINS	Automatic-In-Service state	No Action
IS-AUTO	Automatic OOS-MA to IS	No Action
* *TCA = Threshold Crossing Alert.*		

Alarm/Condition – AIS

6 Retrieve alarms and determine direction of AIS alarm [DLP-100].

7 What is the direction of the alarm?

If Receive (or blank), go to step 10.
If Transmit, go to step 8.

8 ***NOTE:*** *Direction = Transmit: AIS is received on incoming signal (input, demux direction) from SONET network.*

Troubleshoot far-end NE where DS1 facility enters SONET network.

9 STOP. This procedure is complete.

10 ***NOTE:*** *Direction = Receive: AIS is received on incoming (input, mux direction) DS1 facility.*

Troubleshoot far end equipment.

11 STOP. This procedure is complete.

Alarm/Condition – BERL-HT

12 Are there any other DS1 alarms [DLP-100]?

If yes, return to step 5 and resolve other DS1 alarms first.
If no, go to step 13.

13 Check equalization at local LTE per vendor's documentation. Correct if necessary.

NOTE: *Line equalization is applied in the transmit direction. An incorrect equalization setting at the local LTE may cause bit errors at the local (alarmed) NE.*

14 Was equalization correct at local LTE?

If yes, go to step 17.
If no, go to step 15.

15 Change equalization; then retrieve alarms [DLP-100].

16 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 17.

17 From Table A, determine which VTG the alarmed DS1 is on.

18 **CAUTION: Possibility of service interruption. Follow the procedures in DLP-101 when replacing the VTG to avoid loss of traffic.**

19 Replace VTG per DLP-101; then retrieve alarms [DLP-100].

20 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 21.

21 Test the DS1 line per local practice.

22 STOP. This procedure is complete.

Alarm/Condition – DS1ISD

23 Is the alarmed DS1 used to carry traffic?

If yes, go to step 24.
If no, STOP. This procedure is complete (ignore alarm).

24 Check far end to determine if/why a DS1ISD alarm is being generated. If alarm persists, determine/verify that the facilities are cross-connected to the DS1 with the alarm.

25 STOP. This procedure is complete.

Alarm/Condition – INHLPBK

26 To clear alarm, allow remote activation of loopbacks on DS1 facility [DLP-548].

27 STOP. This procedure is complete.

Alarm/Condition – INHPMREPT

28 To clear alarm, allow PM reporting on DS1 facility [DLP-510].

29 STOP. This procedure is complete.

Alarm/Condition – LOS

30 Retrieve alarms and determine direction of LOS alarm [DLP-100].

31 What is the direction of the alarm?

If Receive (or blank), go to step 33.
If Transmit, go to step 32.

32 **NOTE:** *Transmit direction means LOS is detected in the demux direction from the SONET network.*

Go to step 36.

33 **NOTE:** *Receive direction means LOS is detected in the mux direction from the DS1 facility.*

Verify that there are good R/T terminal wire-wrap connections on the IN circuit of the alarmed DS1. (See Figure 1 to find location of alarmed DS1 on shelf backplane.)

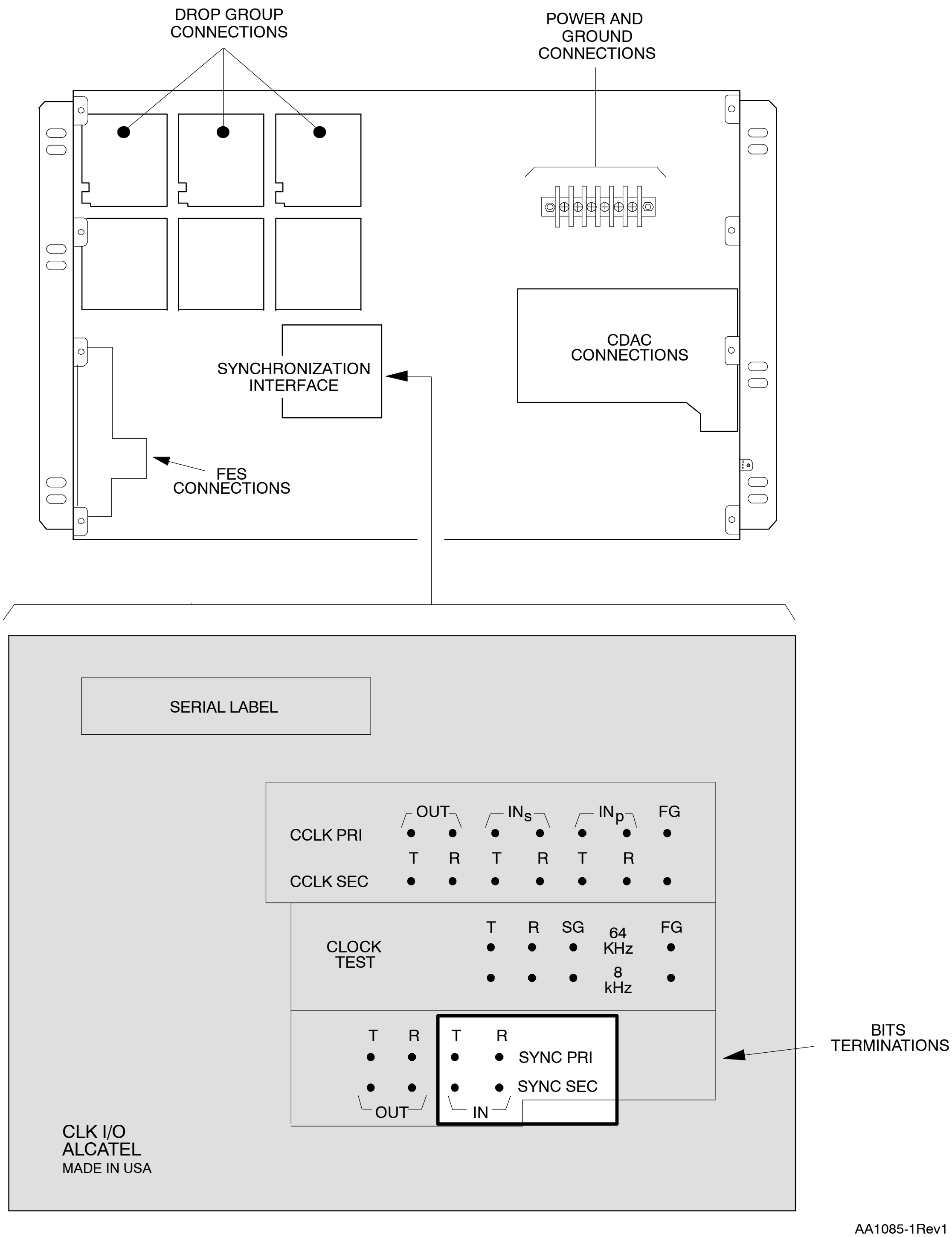


Figure 1. DS1 Wire-wrap I/O Panel Layout

34 Are the connections good?

If yes, go to step 36.
If no, correct the wire-wrap connections.

35 STOP. This procedure is complete.

36 From Table A, determine the VTG carrying the alarmed DS1.

37 Determine VTG service state [DLP-501].

38 From the response, is the VTG unit carrying the alarmed DS1 active (ACT)?

If yes, go to step 40.
If no (STBY), go to step 39.

39 ***NOTE:*** *A faulty VTG caused a switch to protection and may have caused an LOS.*

Go to step 46 to replace VTG.

40 ***NOTE:*** *When an LOS is received, a diagnostic is automatically executed to verify a hard LOS or determine if the VTG is bad.*

Do you want to perform a diagnostic test for LOS?

If yes, go to step 41.
If no, go to step 50.

41 **CAUTION: Possibility of service interruption. The following diagnostics are service-affecting if performed on active VTG.**

42 Place VTG carrying alarmed DS1 in maintenance state [DLP-501].

43 Switch working VTG to protection [DLP-529].

44 Run diagnostic Phase 14 (SA, VTG LOS) on VTG [DLP-500]. Perform 5 iterations.

45 Did diagnostics pass?

If yes, go to step 48.
If no, go to step 46.

46 **CAUTION: Possibility of service interruption. Follow the procedures in DLP-101 when replacing the VTG to avoid loss of traffic.**

47 Replace VTG per DLP-101.

48 Place VTG back in-service [DLP-501].

49 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 50.

50 Is the direction of the alarm receive or transmit?

If receive, go to step 51.
If transmit, go to step 52.

51 Test the DS1 facility; then go to step 53.

52 Check for alarms in the network [DLP-100].

53 STOP. This procedure is complete.

Alarm/Condition – LOF

54 Retrieve alarms and determine direction of LOF alarm [DLP-100].

55 What is the direction of the alarm?

If Receive (or blank), go to step 66.
If Transmit, go to step 56.

LOF – NEND, TRMT Direction

56 Check the provisioning of the DS1 Frame Format parameter and Line Code parameter at the near-end NE and far-end NE [DLP-524].

57 Are Line Code and DS1 Format parameters the same at both ends of the facility?

If yes, go to step 60.
If no, go to step 58.

58 Determine the correct parameter settings from office records and change the parameter(s) that is not correct [DLP-524].

NOTE: *The ESF and SF formats require DMI301.*

59 STOP. This procedure is complete.

60 Check equalization at remote LTE per vendor's documentation. Correct if necessary.

NOTE: *Line equalization is applied in the transmit direction. An incorrect equalization setting at the remote LTE may cause LOF at the remote NE (RCV direction) and local (alarmed) NE (TRMT direction).*

61 Was equalization correct at local LTE?

If yes, go to step 64.
If no, go to step 62.

62 Change equalization; then retrieve alarms at far-end NE [DLP-100].

63 Did LOF alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 64.

64 Are there any equipment or DS1 alarms at far-end NE?

If yes, resolve alarms at far-end NE [TAP-001].
If no, go to step 76.

65 STOP. This procedure is complete.

LOF – NEND, RCV Direction

66 Check the provisioning of the DS1 Frame Format parameter and Line Code parameter at the near-end NE and far-end NE [DLP-524].

67 Are Line Code and DS1 Frame Format parameters the same at both ends of facility?

If yes, go to step 70.
If no, go to step 68.

68 Determine the correct parameter settings from office records and change the parameter(s) that is not correct [DLP-524].

NOTE: *The ESF and SF formats require DMI301.*

69 STOP. This procedure is complete.

70 Check equalization at local LTE per vendor's documentation. Correct if necessary.

NOTE: *Line equalization is applied in the transmit direction. An incorrect equalization setting at the local LTE may cause LOF at the local NE (RCV direction) and remote NE (TRMT direction).*

71 Did LOF alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 72.

72 See Figure 1 to find location of alarmed DS1 on shelf backplane.

73 Verify that R/T terminal wire-wrap connections are good on the IN circuit of the alarmed DS1.

74 Are the connections good?

If yes, go to step 76.
If no, fix the wire-wrap connections.

75 STOP. This procedure is complete.

76 From Table A, determine which VTG is carrying the alarmed DS1.

77 Determine VTG service state [DLP-501].

78 From the response, is the VTG unit carrying the alarmed DS1 active (ACT)?

If yes, go to step 80.
If no (STBY), go to step 79.

79 ***NOTE:*** *A faulty VTG caused a switch to protection and may have caused an LOF.*

Go to step 85 to replace VTG.

80 **CAUTION: Possibility of service interruption. The following diagnostics are service-affecting if performed on active VTG.**

81 Place VTG carrying alarmed DS1 in maintenance state [DLP-501].

82 Switch working VTG to protection [DLP-529].

83 Run all diagnostic phases on VTG [DLP-500]. Perform one iteration.

84 Did diagnostics pass?

If yes, go to step 88.
If no, go to step 85.

85 **CAUTION: Possibility of service interruption. Follow the procedures in DLP-101 when replacing the VTG to avoid loss of traffic.**

86 Replace VTG per DLP-101.

87 Did LOF alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 89.

88 Place VTG back in-service [DLP-501].

89 Per local practice, if Direction=Receive, test the DS1 facility; if Direction=Transmit, look for alarms in the network.

90 STOP. This procedure is complete.

Alarm/Condition – MTCE

91 To clear alarm, place DS1 back in-service [DLP-501].

92 STOP. This procedure is complete.

Alarm/Condition – RAI

93 Retrieve alarms and determine direction of RAI alarm [DLP-100].

94 What is the direction of the alarm?

If Receive (or blank), go to step 95.
If Transmit, go to step 96.

95 RAI is received on incoming (input, mux direction) DS1 facility. Troubleshoot far-end equipment; then go to step 97.

96 ***NOTE:*** *RAI is received on incoming signal (input, demux direction) from SONET network.*

Troubleshoot far-end NE where DS1 facility enters SONET network.

97 Did alarm clear (may take several minutes to clear)?

If yes, STOP. This procedure is complete.
If no, go to step 80 and diagnose VTG at near end.

98 STOP. This procedure is complete.

Alarm/Condition – T-xxx

99 Retrieve current conditions for DS1 facility [DLP-100].

100 Are there any other facility alarms (besides T-xxx)?

If yes, go to step 101.
If no, go to step 102.

101 Correct facility alarms before resolving TCA conditions per Table C.

Table C. DS1 (T1) PM Thresholds

MONITOR TYPE	FACTORY DEFAULT 15-MIN	FACTORY DEFAULT 1-DAY	RANGE	DESCRIPTION
BERL-HT	4		3...6	Bit error ratio line – High threshold (SFBER)
BPV	13340	133400	1...4,294,967,295	Bipolar violations
CSSP	1	4	1...65535	Controlled slips
CVL	13340	133400	1...4,294,967,295	Coding violation count – Line
CVP (FMT=SF)	72	691	1...4,294,967,295	Coding violation count – Path
CVP (FMT=ESF)	13296	132960	1...4,294,967,295	Coding violation count – Path
ESL	65	648	1...65535	Line Errored Seconds
ESP	65	648	1...65535	Path Errored Seconds
SASP	2	17	1...65535	Path AIS seconds
SEFS	2	17	1...65535	Severely errored framing seconds (OOFS/COFAS)
SESL	10	100	1...65535	Line Severely Errored Seconds
SESP	10	100	1...65535	Path Severely Errored Seconds
UASP	10	10	1...65535	Unavailable seconds – Path

102 Is the condition severe enough to warrant unit replacement?

If yes, go to step 104.
If no, record alarm as an event.

103 STOP. This procedure is complete.

104 From the Monitor Conditions work view opened in step 99, determine Location and Direction of T-xxx condition. (See Figure 2 for definition of Location and Direction parameters.)

105 Refer to Table D for corrective action based on location and direction of TCA. See Figure 2 for definition of terms (i.e., NEND, FEND, RCV, and TRMT) used in the table.

Table D. Troubleshooting DS1 TCA Conditions

LOCATION/ DIRECTION	DESCRIPTION	GO TO
NEND/RCV	Suspect local DS1 facility or LTE. Troubleshoot per local practice	Step 106
NEND/TRMT	Suspect network between local and remote NEs. Look for other alarms in SONET network	TAP-001
FEND/RCV	Suspect local DS1 facility or NE. Troubleshoot facility per local practice. If facility is OK, problem may be at local NE	Step 106
FEND/TRMT	Suspect remote DS1 facility or NE. Troubleshoot facility per local practice. If facility is OK, problem may be at remote NE	TAP-001

106 Was problem found and corrected in the facility?

If yes, STOP. This procedure is complete.
If no, go to step 107.

107 Retrieve alarms at the local NE [DLP-100].

108 Are there any CLK or SYNCN alarms?

If there is a CLK alarm, go to TAP-021.
If there is a SYNCN alarm, go to TAP-027.
If neither entity is generating an alarm, go to step 109.

109 Is an HIF, DMI, or VTG unit reporting a SYNCCLK alarm?

If yes, go to TAP-021.
If no, go to step 110.

110 See Figure 1 to find location of alarmed DS1 on shelf backplane.

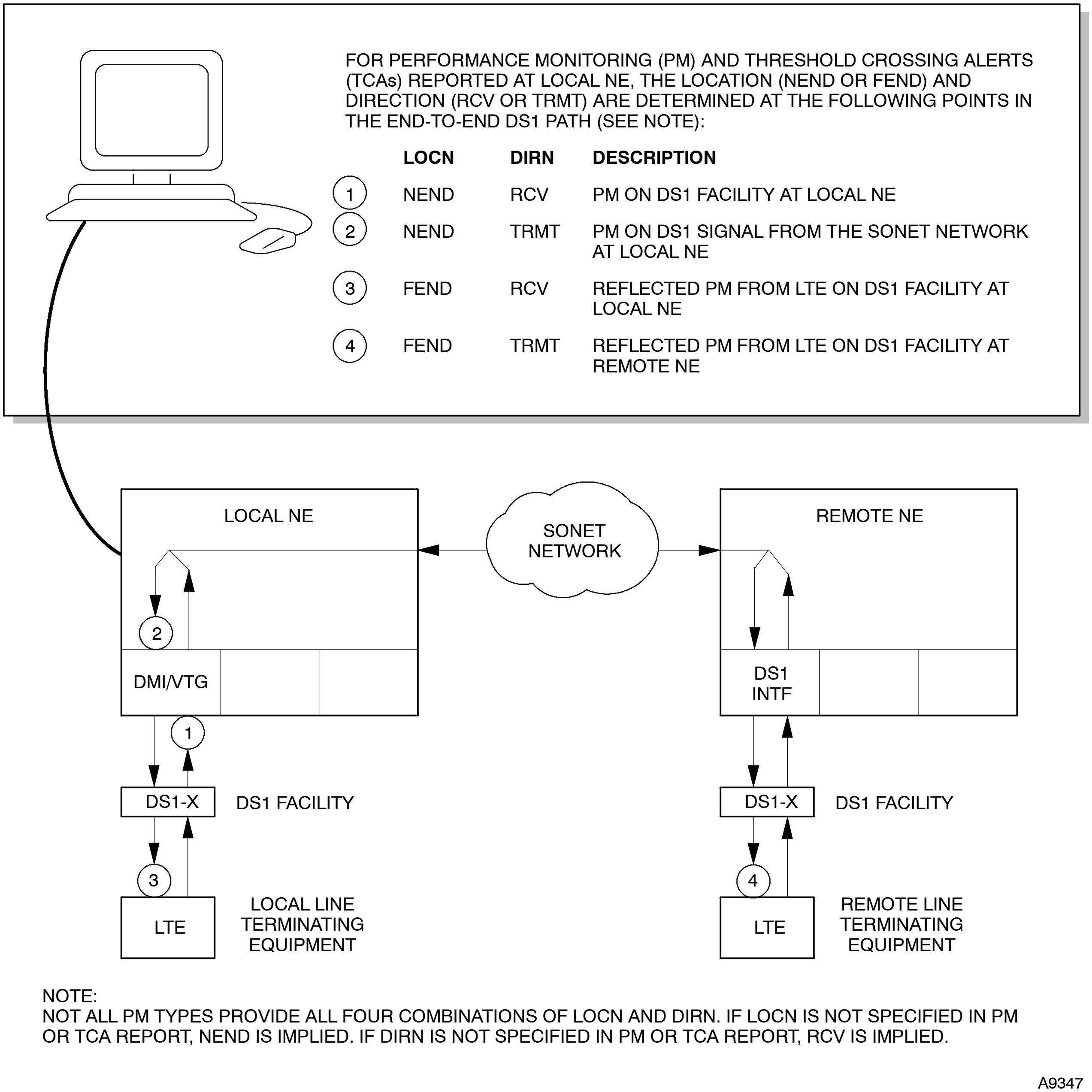


Figure 2. PM Monitoring Points in DS1 Circuit

111 Verify that R/T terminal wire-wrap connections are good for the alarmed DS1.

112 Are the connections good?

If yes, go to step 114.
If no, fix the wire-wrap connections.

113 STOP. This procedure is complete.

114 Verify that the DS1 Frame Format and Line Code parameters are set correctly [DLP-524].

NOTE: *It is not necessary to verify the Frame Format parameter for the following alarms: T-CVL, T-BPV, and T-SESL.*

115 Are Line Code and Frame Format parameters set correctly?

If yes, go to step 118.
If no, go to step 116.

116 Determine correct parameters from office records and reprovision the incorrect DS1 port [DLP-524].

NOTE: *The ESF and SF formats require DMI301.*

117 STOP. This procedure is complete.

118 **CAUTION: Possibility of service interruption. Follow the procedures in DLP-101 when replacing the VTG to avoid loss of traffic.**

119 Replace VTG per DLP-101.

120 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

121 Did PM error stop?

If yes, STOP. This procedure is complete.
If no, go to step 122.

122 Contact Customer Service.

123 STOP. This procedure is complete.

TAP-038
Clear VT1.5 Path Alarm

Purpose

Provides procedures for clearing VT1.5 path alarm.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	**NOTE:** *For VT1 path alarms, supporting equipment, facilities and STS1 path are suspected first.* Perform steps 2 through 8 at each NE in the network before proceeding to step 9.
2	Retrieve alarms [DLP-100].
3	Are there any equipment alarms? If yes, go to step 4. If no, go to step 7.
4	**NOTE:** *All unit alarms are indicated on the COA unit by severity level (CR [Critical], MJ [Major], or MN [Minor]). If there is a COA CONTCOM and an NEP alarm, resolve the COA alarm first.* Identify the alarmed unit with the highest severity.
5	Go to TAP-021 to clear equipment alarms.
6	STOP. This procedure is complete.
7	Are there any parent facility alarms? If OC3, OC12, or OC48, go to TAP-029. If EC1, go to TAP-022. If DS1 (DMI), go to TAP-035. If DS1 (DS3/DS1 Transmux), go to TAP-050. If no parent facility alarms, go to step 8.

8 Are there any parent STS1 alarms?

If yes, go to TAP-034.
If no, go to step 9.

9 Have VT1 path alarms and conditions been retrieved?

If yes, go to step 14.
If no, go to step 10.

10 Retrieve VT1 current conditions [DLP-100].

11 Is location identified on work view?

If yes, go to step 12.
If no (NEND is implied), go to step 14.

12 Is location FEND or NEND?

If FEND, go to step 13.
If NEND, go to step 14.

13 Go to the far-end NE (NE where VT1 path is dropped or terminated) and return to step 1.

14 Identify Access Identifier (refer to Table A).

Table A. DS1 (T1)-to-VT1 Assignment (Sequential and Grouped AID Formats*)

	VTG 1				**VTG 2**				**VTG 3**				**VTG 4**				**VTG 5**				**VTG 6**				**VTG 7**			
T1 SEQ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
VT1.5 SEQ	1	8	15	22	2	9	16	23	3	10	17	24	4	11	18	25	5	12	19	26	6	13	20	27	7	14	21	28
VT1.5 and T1 GRP	1-1	1-2	1-3	1-4	2-1	2-2	2-3	2-4	3-1	3-2	3-3	3-4	4-1	4-2	4-3	4-4	5-1	5-2	5-3	5-4	6-1	6-2	6-3	6-4	7-1	7-2	7-3	7-4

* *The AID format used is determined by the setting of the VT1.5/DS1 Numbering Format parameter (System>General>Global Settings).*

15 Locate alarm or condition in Table B; then go to step indicated to clear it.

Table B. VT Path Alarms/Conditions/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
AISP (rcv and trmt)	Alarm Indication Signal - Path. An upstream failure has occurred. The AISP typically indicates that an upstream NE has inserted AIS into the VT1 path to switch downstream cross-connect selectors away from a failure, unterminated path, or removed facility.	16
BERP-HT	Bit Error Ratio Path-High Threshold. A bit error ratio has exceeded a threshold setting. Signal failure is imminent.	28
BERP-LT	Bit Error Ratio Path-Low Threshold. The number of bits in error to the number of bits received has degraded to the point of exceeding a set threshold. The signal is degraded.	28
FRCD	Forced switch request. A forced path switch has been done on a ring path selector from the line group or drop group specified in the alarm message or response.	42
INHPMREPT	Autonomous reporting of all scheduled PM reports has been inhibited on the VT1.5 path.	45
LOCKOUT	Locked out of protection. A locked-out path switch has been done on a ring path selector from the line group or drop group specified in the alarm message or response.	42
LOP (rcv and trmt)	Loss of Pointer. A valid pointer cannot be obtained for the VT SPE to the STS SPE alignment.	47
MAN	Manual switch request. A manual path switch has been done on a ring path selector from the line group or drop group specified in the alarm message or response.	51
PATHSEL	Path Selector. Problems on both rings caused the ring path selector to fail and interrupt traffic.	16
PLM (rcv and trmt)	Payload Label Mismatch. The content of the SONET V5 byte is inconsistent or invalid. Probable causes for this condition are the incoming payload type is incorrect due to network routing problems or the expected VT signal label is provisioned incorrectly.	53
PROTNA	Protection Not Available. Service interruption may occur if active ring path fails because there is no protection path available.	16
RFI	VT path yellow detected	60
T-CVP	VT Coding Violation - Path TCA. (NEND RCV or FEND RCV)	63

Table B.   VT Path Alarms/Conditions/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
T-ESP	VT Errored Seconds – Path TCA. (NEND RCV or FEND RCV)	63
T-NPJCDET	Negative Pointer Justification Count Detected TCA	63
T-NPJCGEN	Negative Pointer Justification Count Generated TCA	63
T-PPJCDET	Positive Pointer Justification Count Detected TCA	63
T-PPJCGEN	Positive Pointer Justification Count Generated TCA	63
T-PJCSDET	Pointer Justification Count Seconds Detected TCA	63
T-PJCSGEN	Pointer Justification Count Seconds Generated TCA	63
T-PJCSDIFF	Pointer Justification Count Difference TCA	63
T-SESP	Severely Errored Seconds – Path TCA (NEND RCV or FEND RCV)	63
T-UASP	Unavailable Seconds – Path TCA (NEND RCV or FEND RCV)	63
UNEQ (rcv and trmt)	Unequipped. The VT1 is receiving a signal label value of 0 (unequipped).	158
VTSIZE	The VT size (VT6, VT3, VT2, or VT1.5) received from the far-end NE is different from what is equipped or provisioned. The 1603 SMX currently only supports VT1.5 size payloads. Far-end drop group is most likely connected to incorrect type of facility.	161
Condition	**Description**	**Action**
SIGLBL- xxx where xxx = 1...255	VT path signal label. xxx is the signal label code received in the V5 byte	No Action
TSA-n	Test session active, where: n = MONE, MONF, SPLTA, SPLTB, SPLTE, SPLTF, LOOPE, LOOPF	No Action
TSN-n	Test session number, where n = 1...999	No Action
If VT1.5 path is in a drop group and is cross-connected to a ring path selector (1WAYPR, 2WAYPR, 2WAYBR), the following non-alarmed conditions are added.		
PROTECTED-ACT	Protected path is active	No Action
PROTECTING-ACT	Protecting path is active	No Action
PROTECTED-ALL	Protected path conditions (TL1 input only)	No Action
PROTECTING-ALL	Protecting path conditions (TL1 input only)	No Action
PROTECTED-DG1/DG1A/DG1B	Protected path is Drop Group 1, Drop Group 1A, or Drop Group 1B	No Action
PROTECTING-DG1/DG1A/DG1B	Protecting path is Drop Group 1, Drop Group 1A, or Drop Group 1B	No Action

Table B. VT Path Alarms/Conditions/Events (cont)

Condition	Description	Action
PROTECTED-DG2/DG2A/ DG2B	Protected path is Drop Group 2, Drop Group 2A, or Drop Group 2B	No Action
PROTECTING-DG2/DG2A /DG2B	Protecting path is Drop Group 2, Drop Group 2A, or Drop Group 2B	No Action
PROTECTED-DG3/DG3A/ DG3B	Protected path is Drop Group 3, Drop Group 3A, or Drop Group 3B	No Action
PROTECTING-DG3/DG3A /DG3B	Protecting path is Drop Group 3, Drop Group 3A, or Drop Group 3B	No Action
PROTECTED-DG4/DG4A/ DG4B	Protected path is Drop Group 4, Drop Group 4A, or Drop Group 4B	No Action
PROTECTING-DG4/DG4A /DG4B	Protecting path is Drop Group 4, Drop Group 4A, or Drop Group 4B	No Action
PROTECTED-FAIL	Protected path fails	*
PROTECTING-FAIL	Protecting path fails	*
PROTECTED-FRCD	Forced switch requested on protected path	*
PROTECTING-FRCD	Forced switch requested on protecting path	*
PROTECTED-LG1	Protected path is Line Group 1	No Action
PROTECTING-LG1	Protecting path is Line Group 1	No Action
PROTECTED-LG2	Protected path is Line Group 2	No Action
PROTECTING-LG2	Protecting path is Line Group 2	No Action
PROTECTED-LOCKOUT	Protected path is lockout of protection	*
PROTECTING-LOCKOUT	Protecting path is lockout of protection	*
PROTECTED-MAN	Manual switch requested on protected path	*
PROTECTING-MAN	Manual switch requested on protecting path	*
PROTECTED-RFI	Protected path is VT1.5 path yellow	*
PROTECTING-RFI	Protecting path is VT1.5 path yellow	*
PROTECTED-STBY	Protected path is standby	No Action
PROTECTING-STBY	Protecting path is standby	No Action
PROTECTED-UNEQ	Protected path is unequipped	*
PROTECTING-UNEQ	Protecting path is unequipped	*
Event	**Description**	**Action**
WTRREVERT	Wait to revert time-out, reported as switch reason	*
FRCDWKSWBK	Protected path forced switch back	No Action
FRCDWKSWPR	Protected path forced switch to prot.	No Action

Table B. VT Path Alarms/Conditions/Events (cont)

Event	Description	Action
MANWKSWBK	Manual switch of protected back	No Action
MANWKSWPR	Manual switch of protected to protecting	No Action
WKSWBK	Protected path switch back	No Action
WKSWPR	Protected path switch to protection	No Action
* *Look for and troubleshoot related VT1.5 alarms.*		

Alarm/Condition – AISP, PATHSEL or PROTNA

16 ***NOTE:*** *PATHSEL and PROTNA alarms could be caused by any of the following conditions: an upstream failure has occurred; a facility is removed or unassigned; or network VT1 cross-connections in both paths are not in place.*

Perform steps 17 thru 25 at each NE in the network. Start with the nearest NE.

17 Retrieve alarms [DLP-100].

18 Are there any equipment alarms?

If yes, go to TAP-021.
If no, go to step 19.

19 Are there any facility alarms?

If yes, resolve alarms per TAP-001.
If no, go to step 20.

20 Retrieve cross-connection for VT1 path [DLP-504].

21 Is the cross-connection for VT1 path in place?

If yes, go to step 25.
If no, go to step 22.

22 Re-establish VT1 path cross-connect [DLP-504].

23 Does path terminate on LIF601?

If yes, go to step 24.
If no, go to step 25.

24 Verify DS3/DS1 TransMux facility is in-service. If out-of-service or in maintenance state, place facility in-service [DLP-501]; then go to step 26.

25 Verify parent facilities are in-service. If out-of-service or in maintenance state, place facility in-service [DLP-501].

26 Have all NEs been checked?

If no, select next NE in network; then return to step 17.
If yes, go to step 27.

27 STOP. This procedure is complete.

Alarm/Condition – BERP-HT or BERP-LT

28 Retrieve alarms [DLP-100].

29 Are there any equipment alarms?

If yes, clear these alarms per TAP-029; then go to step 31.
If no, go to step 30.

30 Are there any facility alarms?

If yes, clear these alarms per TAP-001; then go to step 31.
If no, go to step 33.

31 Retrieve VT alarms [DLP-100].

32 Did BERP-HT or BERP-LT alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 33.

33 Switch redundant CCMs [DLP-505]; then retrieve VT alarms [DLP-100].

34 Did BERP-HT or BERP-LT alarm clear (may take several minutes)?

If yes, go to step 35.
If no, go to step 38.

35 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing the CCM unit to avoid service interruption.**

36 Replace the standby CCM unit per DLP-101; then retrieve alarms [DLP-100].

37 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 38.

38 Problem must be at far-end terminal. Analyze and clear far-end NE alarms. Refer to TAP-001.

39 Did clearing alarms at far-end NE clear BERP-HT/BERP-LT alarm?

If yes, STOP. This procedure is complete.
If no, go to step 40.

40 If problem persists, test fiber facility as specified by local procedure.

41 STOP. This procedure is complete.

Alarm/Condition – FRCD or LOCKOUT

42 **CAUTION: Possibility of service interruption. The FRCD/LOCKOUT condition should not be allowed under normal conditions. This condition prevents the path selector from automatically switching to the protecting path if a failure occurs in the ring network requiring the selector to switch, which would interrupt service.**

43 ***NOTE:*** *If revertive switching is not enabled, the switch can be released and the selected path remains active.*

To clear alarm, release protection switching [DLP-507].

44 STOP. This procedure is complete.

Alarm/Condition – INHPMREPT

45 To clear alarm, allow PM reporting on VT1.5 path [DLP-510].

46 STOP. This procedure is complete.

Alarm/Condition – LOP

47 Retrieve alarms [DLP-100].

48 Are there any equipment or facility alarms?

If yes, resolve these alarms first. Refer to TAP-021 (equipment) or TAP-001 (facility).
If no, go to step 49.

49 Use the same steps for clearing an AISP alarm, but substitute LOP wherever AISP is used. Go to step 16.

50 STOP. This procedure is complete.

Alarm/Condition – MAN

51 ***NOTE:*** *The MAN condition is the lowest priority level and does not affect service if left active; however the alarm remains. If revertive switching is not enabled, the switch can be released and the selected path remains active.*

To clear the alarm, release protection switching [DLP-507].

52 STOP. This procedure is complete.

Alarm/Condition – PLM

53 See Figure 1 for signal label monitoring points in the 1603 SMX Network Element.

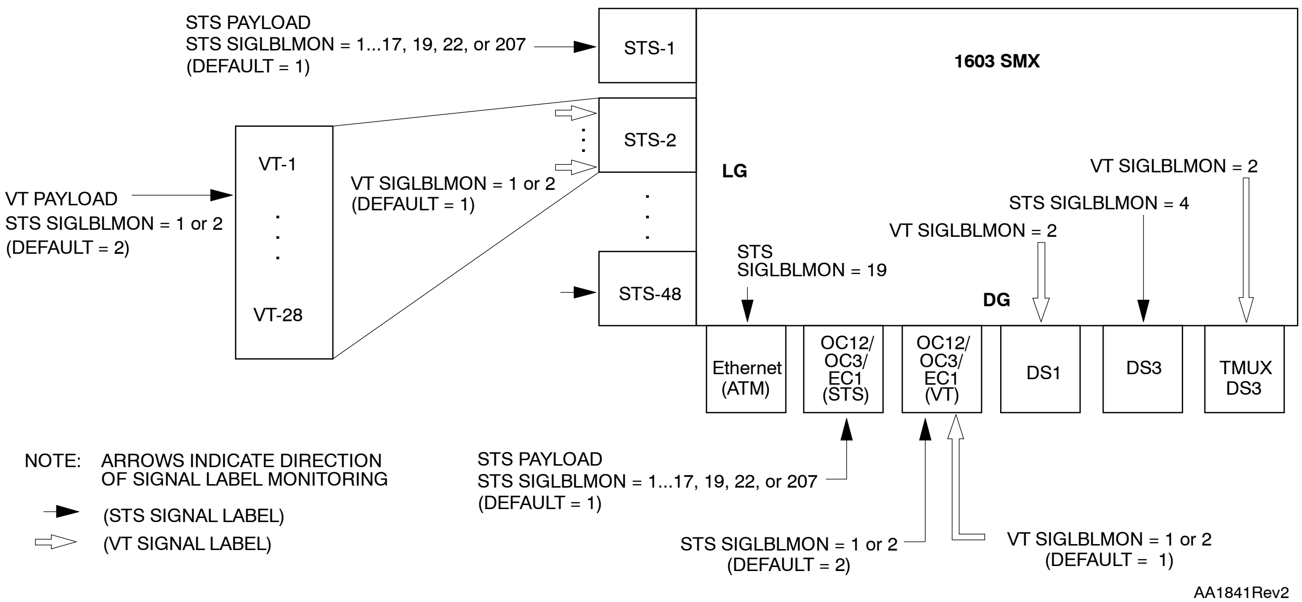


Figure 1. Signal Label Monitoring – STS (C2 Byte) and VT (V5 Byte)

54 Retrieve VT1 conditions [DLP-100].

55 To determine the incoming signal label, which is in the V5 byte, locate SIGLBL-xxx in the Condition column on the Monitor Conditions work view.

56 Note the number following SIGLBL; then find that number in Table C to identify the contents of the VT1 Synchronous Payload Envelope (SPE).

Table C. VT Path Signal Label Assignments*

BYTE V5CODE	CONTENTS OF VT SPE
0	Unequipped
1	Equipped – nonspecific payload
2	Asynchronous mapping for DS1

* *From BellCore Document GR-253-CORE, Issue 2, Dec. 1995. Note that values not listed are not defined.*

57 Determine the expected (provisioned) VT1 signal label [DLP-509].

58 Compare the incoming signal label (step 56) and expected signal label (step 57). Determine which is correct. Refer to Table D for recommended corrective action.

59 STOP. This procedure is complete.

Table D. Clearing VT1 Payload Label Mismatch (PLM) Alarm

LOCATION OF PLM ALARM	PROBABLE CAUSES	RECOMMENDED ACTIONS
Line or Drop Group – Unterminated VT1 Allowed values of expected VT Signal label = 1 or 2	Payload type indication in incoming V5 byte is incorrect	Check network cross-connections and change if necessary [DLP-504]. Check payload type at path origin and change if necessary [DLP-511].
	Expected VT1 Signal Label parameter is incorrectly provisioned	Change expected VT1 signal label parameter to reflect the signal label in V5 byte [DLP-509].
Drop Group – DS1 – Terminated VT1 Expected VT1 Signal label = 2* (not provisionable)	Payload type indication in incoming V5 byte is incorrect	Check network cross-connections and change if necessary [DLP-504]. Check payload type at path origin and change if necessary [DLP-511].
* *AIS is inserted on DS1 payload.*		

Alarm/Condition – RFI

60 ***NOTE:*** *A failure was detected along the downstream STS path. Probable causes are equipment or facility problems at this NE or between this NE and the far-end NE that terminates this path.*

See Figure 2 for a probable scenario.

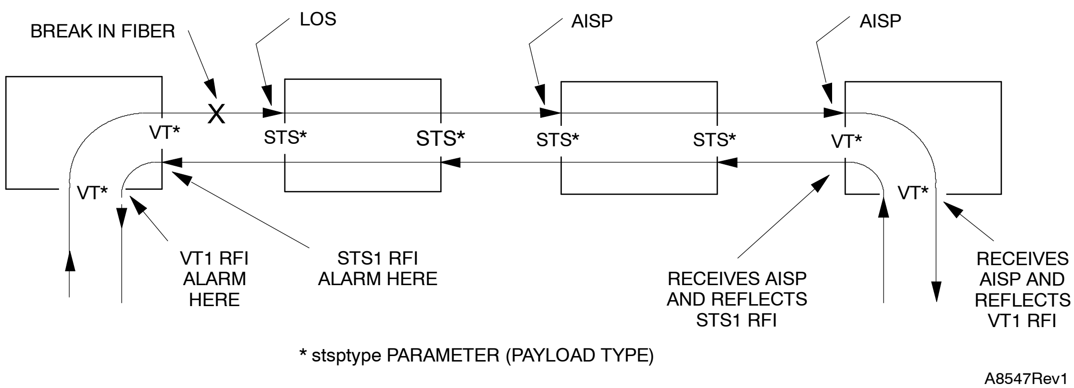


Figure 2. Example Network

61 Look for and clear other alarms in the network. Refer to TAP-001.

62 STOP. This procedure is complete.

Alarm/Condition – T-xxx

NOTE: *A threshold crossover alert has been generated because one of the performance parameters exceeds the value specified for it. As a default, these conditions are not reported as an alarm, but as an event, unless the attribute has been changed to minor (MN), major (MJ), or critical (CR). Refer to Table E.*

These conditions indicate different levels of path degradation.

The path layer transports the network services between SONET terminal multiplexing equipment (DS1s). It maps the services into the format required for the line layer.

63 Is the condition severe enough to warrant unit replacement?

If yes, go to step 66.
If no, go to step 64.

64 Record the alarm as an event.

65 STOP. This procedure is complete.

Table E. VT1 PM Thresholds

MONITOR TYPE	FACTORY DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERP-HT	4		3...4	Bit Error Ratio Path — High threshold (SFBER)
BERP-LT	6		5...8	Bit Error Ratio Path — Low threshold (DGBER)
CVP	15	146	1...4,294,967,295	Coding Violation Count — path (near end or far end)
DSESP	600		1...65535	Number of coding violations to make one SESP
ESP	12	117	1...65535	Path Error Second (near end or far end)
NPJCDET	2	192	1...4,294,967,295	Negative Pointer Justification Count Detected
NPJCGEN*	2	192	1...4,294,967,295	Negative Pointer Justification Count Generated
PPJCDET	2	192	1...4,294,967,295	Positive Pointer Justification Count Detected
PPJCGEN*	2	192	1...4,294,967,295	Positive Pointer Justification Count Generated
PJCSDET	2	192	1...65535	Positive Justification Count Seconds Detected
PJCSGEN	2	192	1...65535	Positive Justification Count Seconds Generated
PJCDIFF	2	192	1...4,294,967,295	Pointer Justification Count Difference
SESP	3	7	1...65535	Path Severely Errored Seconds (near end or far end)
UASP	10	10	1...65535	Path Unavailable Seconds (near end or far end)

* *The range for LIF601 and DMI equipped drop groups is 1...65535.*

66 **CAUTION: Possibility of service interruption. Follow the replacement procedure in DLP-101 when replacing plug-in units to avoid loss of traffic.**

67 Retrieve STS1 alarms and conditions [DLP-100].

68 Is there a T-xxx condition on the parent STS1 path?

If yes, go to TAP-034.
If no, go to step 69.

69 Retrieve alarms [DLP-100].

70 Are there any CLK or SYNCN alarms?

If CLK alarms, go to TAP-021.
If SYNCN alarms, go to TAP-027.
If no CLK or SYNCN alarms, go to step 71.

71 Are there any equipment alarms?

If yes, go to step 72.
If no, go to step 75.

72 ***NOTE:*** *All unit alarms are indicated on the COA unit by severity level (Critical [CR], Major [MJ], or Minor [MN]). If there is a COA CONTCOM and an NEP alarm, resolve the COA alarm first.*

Identify the alarmed unit with the highest severity.

73 Go to TAP-021 to clear equipment alarms.

74 STOP. This procedure is complete.

75 Is threshold event in an OC3, OC12, or OC48 facility?

If yes, go to step 80.
If no, go to step 76.

76 Is drop group equipped with DMI or LIF?

If DMI, go to step 77.
If LIF, go to step 83.

77 Replace the VTG associated with threshold crossing per DLP-101.

78 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves register values.*

79 Did PM errors stop?

If yes, STOP. This procedure is complete.
If no, go to step 83 to look for other problems.

80 Replace the OCn HIF or LIF per DLP-101 for the associated line group or drop group.

81 Wait several minutes; then retrieve PM registers again [DLP-517].

82 Did PM errors stop?

If yes, STOP. This procedure is complete.
If no, go to step 83 to look for other problems.

83 ***NOTE:*** *The far end is detecting a problem on the receive (facility) side. Problem is most likely at near-end equipment or on the facility.*

Refer to Table F and locate the type of LIF associated with the facility reporting the alarm. Go to the step referenced in the table to clear the alarm.

Table F. Types of LIFs

IF DROP GROUP IS EQUIPPED WITH AN...	AND UNIT IS...	THEN GO TO...
LIF201	Non-redundant	Step 84
	Redundant	Step 100
LIF501/701	Non-redundant	Step 84
	Redundant	Step 122
LIFD01	Non-redundant	Step 132
	Redundant	Step 146

Non-redundant LIF201 or LIF501/701 Unit

84 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF and LDR units. If facility is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

85 At the near-end NE, place LIF to be diagnosed in maintenance state (OOS-MT-MAN) [DLP-501].

86 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

87 Did diagnostics pass?

If yes, go to step 90.
If no, go to step 88.

88 Replace LIF per DLP-101.

89 STOP. This procedure is complete.

90 Place LIF back in-service [DLP-501].

91 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR.**

92 Place LDR to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

93 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

94 Did diagnostics pass?

If yes, go to step 97.
If no, go to step 95.

95 Replace LDR per DLP-101.

96 STOP. This procedure is complete.

97 Place LDR back in-service [DLP-501].

98 Problem most likely in facility. Troubleshoot per local practice.

99 STOP. This procedure is complete.

Redundant LIF201 Unit

The active and standby LIFs will be switched to determine whether the active LIF or active LDR is causing the alarm.

100 Switch to duplex LIF [DLP-505].

NOTE: *When LIF20x units are switched, the LDRs also switch, i.e., LDR-A is active when LIF-A is active, and LDR-B is active when LIF-B is active.*

101 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves register values.*

102 Did PM errors stop?

If yes, go step 105.
If no, go to step 103.

103 Problem most likely in facility. Troubleshoot per local practice.

104 STOP. This procedure is complete.

105 Problem must be in standby LIF or LDR. Go to step 106 and perform diagnostics on LIF.

106 **CAUTION: Possibility of service interruption. Diagnostics are service-affecting if performed on active units. Be sure the LIF and LDR units are in standby before performing diagnostics.**

107 Place LIF to be diagnosed in maintenance state (OOS-MT-MAN) [DLP-501].

108 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

109 Place LIF back in-service [DLP-501].

110 Did diagnostics pass?

If yes, go to step 113.
If no, go to step 111.

111 Replace LIF per DLP-101.

112 STOP. This procedure is complete.

113 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR. Perform the following on standby side if LIF and LDR are duplex. Be sure the LIF and LDR units are in standby before performing diagnostics.**

114 Place LDR to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

115 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

116 Place LDR back in-service [DLP-501].

117 Did diagnostics pass?

If yes, go to step 120.
If no, go to step 118.

118 Replace LDR per DLP-101.

119 STOP. This procedure is complete.

120 Problem most likely in facility. Troubleshoot per local practice.

121 STOP. This procedure is complete.

Redundant LIF501/701 Unit

NOTE: *The active and standby LIFs associated with the alarmed facility will be switched to determine whether the active LIF is causing the alarm. If the alarm isn't cleared, the active and standby LDRs associated with the alarmed facility will be switched.*

122 Switch to duplex LIF [DLP-505].

123 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves register values.*

124 Did PM errors stop?

If yes, replace standby LIF per DLP-101.
If no, go to step 126.

125 STOP. This procedure is complete.

126 Switch to duplex LDR [DLP-505].

127 Wait several minutes; then retrieve PM registers [DLP-517].

128 Did PM errors stop?

If yes, replace standby LDR per DLP-101.
If no, go to step 130.

129 STOP. This procedure is complete.

130 Problem most likely in facility. Troubleshoot per local practice.

131 STOP. This procedure is complete.

Non-Redundant LIFD01 Unit

NOTE: *Diagnostics will be performed on the LIF associated with the alarmed facility. If diagnostics pass, the protection LDR and the LDR associated with the alarmed facility will be switched.*

132 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF unit. If facility is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

133 Place LIF to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

134 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

135 Did diagnostics pass?

If yes, go to step 137.
If no, replace LIF per DLP-101.

136 STOP. This procedure is complete.

137 Place LIF back in-service [DLP-501].

138 Switch the LDR501 that is carrying the alarmed VT1 path to protection [DLP-529]. (For help in identifying the AID of the LDR refer to DLP-565.)

NOTE: *Revertive switch may occur. Inhibit switch back to working if required.*

139 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves register values.*

140 Did PM errors stop?

If yes, go step 141.
If no, go to step 143.

141 Replace the LDR501 that was switched to protection [DLP-101]. (For help in identifying the physical location of the LDR, refer to DLP-565.)

142 STOP. This procedure is complete.

143 If switch back to working was inhibited, allow automatic switching to working unit [DLP-536].

144 Problem most likely in facility. Troubleshoot per local practice.

145 STOP. This procedure is complete.

Redundant LIFD01 Unit

NOTE: *The active and standby LIFs associated with the alarmed facility will be switched to determine whether the active LIF is causing the alarm. If the alarm isn't cleared, the protection LDR and the LDR associated with the alarmed facility will be switched.*

146 Switch to duplex LIF [DLP-505].

147 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves register values.*

148 Did PM errors stop?

If yes, replace standby LIF per DLP-101.
If no, go to step 150.

149 STOP. This procedure is complete.

150 Switch the LDR501 that is carrying the alarmed VT1 path to protection [DLP-529]. (For help in identifying the AID of the LDR refer to DLP-565.)

NOTE: *Revertive switch may occur. Inhibit switch back to working if required.*

151 Wait several minutes; then retrieve PM registers [DLP-517].

152 Did PM errors stop?

If yes, go step 153.
If no, go to step 155.

153 Replace the LDR501 that was switched to protection [DLP-101]. (For help in identifying the physical location of the LDR, refer to DLP-565.)

154 STOP. This procedure is complete.

155 Allow automatic switching to working unit [DLP-536].

156 Problem most likely in facility. Troubleshoot per local practice.

157 STOP. This procedure is complete.

Alarm/Condition – UNEQ

158 Check VT1 level cross-connection at each upstream NE [DLP-504].

159 If problem persists, contact Customer Service.

160 STOP. This procedure is complete.

Alarm/Condition – VTSIZE

161 Retrieve VT1 conditions for group containing alarmed VT1 path [DLP-100].

162 Is there an AISP alarm?

If yes, go to step 16.
If no, go to step 163.

163 Log on to the far-end NE that is supposed to terminate the parent STS1 path of the alarmed VT1 path.

164 Determine STS1 payload type [DLP-511].

165 Is Payload Type = VT?

If yes, go to step 168.
If no, go to step 166.

166 Change payload type to VT [DLP-511].

167 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 168.

168 Look for other alarms per TAP-001. If alarm cannot be isolated, contact Customer Service.

169 STOP. This procedure is complete.

TAP-039 Resolve Craft Communications Loss

Purpose

Provides procedures for troubleshooting a craft communication loss.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	***NOTE:*** *A loss of power at the NE would cause loss of communications with NE plus network alarms at other NE connected to the NE. Also, if the NE is equipped with CCL-B or earlier versions of the PWRA01 power units, the units may be in a protective latched-off mode if the input power momentarily dropped below minimum voltage specifications. In this case, the PWR units need to be reseated to unlatch the units.*
2	Has -48 Vdc power failed? If yes, resolve per local procedures. If no, go to step 3.
3	Is -48 Vdc power within specified requirements, but NE is dead (i.e., loss of all traffic)? If yes, remove PWR units and inspect for signs of physical failures; then go to step 4. If no, go to step 6.
4	Were any units damaged? If yes, replace units; then go to step 5. If no, reinstall PWR units; then go to step 6.
5	Did NE return to normal operations? If yes, STOP. This procedure is complete. If no, go to step 6.
6	Over which port did communications loss occur? If Craft 1 Port, go to step 20. If Craft 2 Port, go to step 38. If remote logon, go to step 7.

Remote Logon Communications Loss

7 Retrieve NE alarms [DLP-100].

8 Are there any equipment alarms?

If yes, go to step 9.
If no, go to step 11.

9 ***NOTE:*** *All unit alarms are indicated on the COA unit by severity level (i.e.,CR [Critical], MJ [Major], or MN [Minor]). If there is a COA CONTCOM and an NEP alarm, resolve the COA alarm first.*

Identify the alarmed unit with the highest severity; then go to TAP-021 to clear equipment alarms.

10 STOP. This procedure is complete.

11 Are there any OCn or SML facility alarms?

If OCn, go to TAP-029.
If SML, go to TAP-033.
If neither OCn or SML, then go to step 12.

12 Are there any lower layer link alarms?

If LLSDCC, go to TAP-032.
If LLSMLDCC, go to TAP-045.
If LAN, go to TAP-044.
If no lower layer link alarms, then go to step 13.

13 Retrieve direct neighbors for NE and determine if a lower layer link is not communicating [DLP-560].

14 Examine the response to determine which link has no connection.

NOTE: *Any link not listed in the table is a link that is not communicating.*

15 Is a link not communicating?

If yes, go to step 16.
If no, go to step 18.

16 ***NOTE:*** *Both ends of the lower-layer link must be in-service (pst=IS) for remote logon capability.*

Verify operations channel provisioning at local and neighboring NEs [DLP-128].

17 STOP. This procedure is complete.

18 Suspect a faulty COA or NEP plug-in unit at local or remote NE. Go to TAP-021.

19 STOP. This procedure is complete.

Craft 1 Port Communication Loss

20 ***NOTE:*** *The Craft 1 port requires a standard RS-232 cable (not null modem). Refer to Table A for cables available from Alcatel.*

Verify cable connections from the terminal or PC to the Craft 1 port (USI connector on the front of the COA).

Table A. RS-232 Cables

DESCRIPTION	PART NUMBER
9-pin Male to 25-pin Female Cable Assembly	601229-540-072
9-pin Male to 25-pin Male Cable Assembly	601154-540-072
9-pin Male to 9-pin Female Cable Assembly	695-7683-033

21 Disconnect the cable on both ends.

22 Inspect for bent or broken pins on the cable connectors, the COA connector, and the terminal connector.

23 Verify cable wiring per Figure 1. Replace cable if faulty or wired incorrectly.

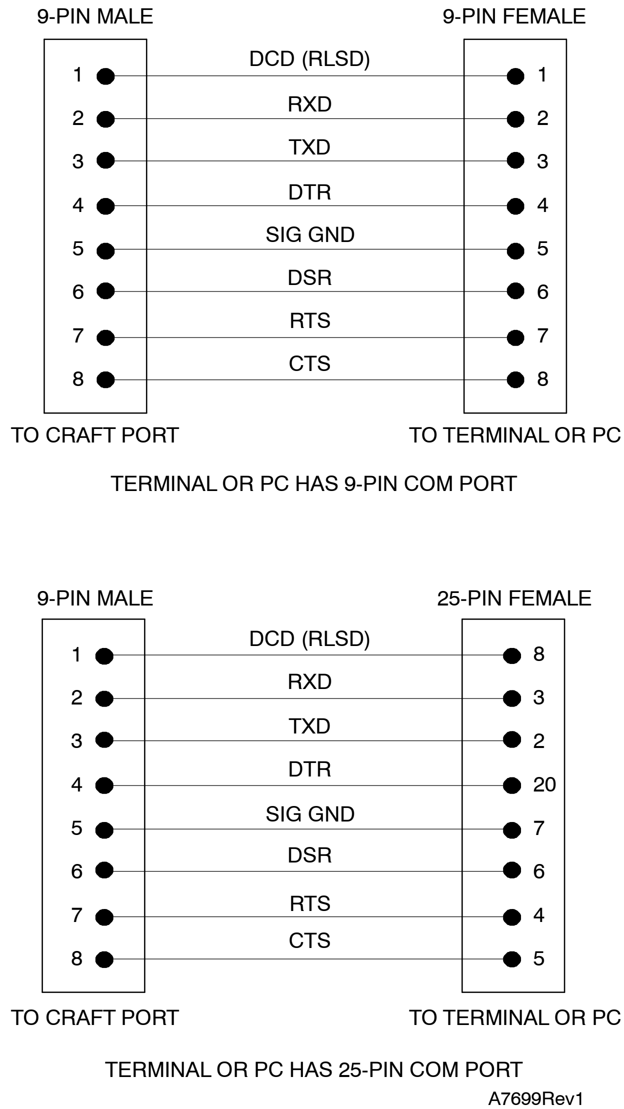


Figure 1. Craft 1 Port Interface Cable Wiring

24 Reconnect cable to Craft 1 port.

25 Is the terminal responding correctly?

If yes, STOP. This procedure is complete.
If no, go to step 26.

26 Go to another NE and perform a remote logon to this NE so you can interrogate the database [DLP-117].

27 Retrieve Craft 1 port parameters [DLP-502].

28 Analyze the port parameters. Refer to Table B and Table C.

29 Compare the Craft 1 port parameters to the communication port settings of the PC terminal emulator program.

30 Are the provisioned port parameters and the PC communications port settings compatible?

If yes, go to step 31.
If no (or do not know), go to step 32.

31 Suspect a faulty COA or NEP plug-in unit. Go to TAP-021.

32 Do you need to modify port parameter settings or PC communications settings?

If PC settings, go to step 33.
If port parameter settings, go to step 34.

33 Change parameters for PC terminal emulator being used (refer to Tables C and D); then go to step 35.

34 Modify the required Craft 1 port parameters [DLP-502].

35 Is communication with NE established?

If yes, STOP. This procedure is complete.
If no, go to step 36.

36 Suspect a faulty COA or NEP plug-in unit. Go to TAP-021.

37 STOP. This procedure is complete.

Table B. Port Parameters

PORT PARAMETERS	DESCRIPTION
Service State	Used to apply a specific service state on the specified craft port. The parameter can be one of the following: IS – In-Service (Input) MA – Memory Administration (Input) MT – Maintenance State (Input) OOS – Out-of-Service (synonomous with MA) (Input)
Stop Bits	Time interval between transmitted characters. Expressed as the number of stop BITS for the craft interface. The parameter value must be 1, 1.5, or 2.
Baud Rate	Data transfer speed for the craft interface. The parameter must match the remote system baud rate. The parameter value can be 300, 1200, 2400, 4800, 9600, 19200 or Autobaud.
Data Bits	The number of data bits sent in each data packet. Referred to as the character size for the craft interface. The parameter value must be: 7 or 8 (bits).
Parity	A self-checking method of minimizing transmission errors in transmit and receive data signals. The parameter value must be NONE (no parity check); ODD (odd parity check); or EVEN (even parity check).
Terminal type	Type of terminal connected to the craft interface. The parameter type must be a VT100 (DEC VT100 compatible device) or a TTY (a hard copy device).
Line Width	Character line width for the craft interface. Any lines with more than the specified line width automatically wrap to the next line on the screen. The parameter must be a value between 10 and 132, inclusive.
Echo	Allows the user to see the outgoing data (keystrokes) on screen when communicating with a remote system. The parameters are Echo on (full duplex) or echo off (half duplex). Half duplex cannot echo keystrokes to the screen, full duplex can (preferred mode).
XON/XOFF Flow Control	Enables or disables XON/XOFF flow control for Craft 1 and Craft 2 port. The parameter should be enabled for 1301 NMX.
Primary State	Current service state of the specified craft port. Allowable parameters are In-Service (Input) In-Service – Abnormal (Response only) In-Service – Normal (Response only) Out-of-Service (synonomous with MA) (Input) Out-of-Service – Assigned (Response only) Out-of-Service – Unassigned (Response only)

Table C. Communications Port Settings Screen Description

FIELD	MEANING	RANGE/CHOICE
Symbol Label	Displays label applied to communications port	Entered data
Port	Specifies communications port being configured	Com 1 through Com 16 Default is COM 1
Baud	Specifies baud rate for port	Recommended rate for modem connection is 9600
Data Format	Three-character format. First character specifies parity for communications port, second character specifies number of bits in a data character, third character specifies number of stop bits used	N-8-1 O-7-1 E-7-1 N-7-2 1301 NMX-1603 SMX default configuration is N-8-1
OK	Applies specified changes and closes the screen	As shown on screen
Cancel	Closes the screen without applying changes	As shown on screen
Help	Accesses 1301 NMX online help for 1603 SMX application	As shown on screen

Table D. Modem Port Setup Screen Description

FIELD	MEANING	RANGE/CHOICE
Symbol Label	Displays Label applied to the Modem Port icon (If Modem Setup: Phone number is entered, same number as label.)	String of alphanumeric characters
Port	Specifies PCs com port being configured for modem to use	Com1 (default) through Com16
Baud	Specifies baud rate for the port. Set this value to match the network element	1200, 2400, 4800 9600 (Recommended) 14400, 19200 (default) 28800, 38400, 57600 115200
Format	Three-character format. Parity - Data Bits - Stop Bits. Set this value to match the network element	N-8-1 (default) (Recommended) O-7-1 E-7-1 N-7-2
Phone Number	Specifies modem number to be dialed for NE access	Entered data
Timeout	Specifies length of time (in seconds) modem allows to dial and make connection; if no connection within this time, modem hangs up	30—600 seconds 60 (default) (Recommended)
Show terminal after connect (optional)	If selected, allows user interaction after connecting with the remote modem but prior to establishing a connection with the target NE. Used for password entry or call-back modem operation.	Selected/Unselected
Modem Init (Optional)	Commands to configure modem before dialing	Hayes-compatible modem command set
Dial Suffix (Optional)	Commands to configure modem after connection has been made	As appropriate per application
OK	Applies the specified changes and closes the setup dialog box	As shown on the screen
Cancel	Closes the window without applying the changes	As shown on the screen
Help	Accesses 1301 NMX online help	As shown on the screen

Craft 2 Port Communication Loss

38 Is Craft 2 wiring for data terminal (DTE) or modem (DCE)?

If data terminal, go to step 39.
If modem, go to step 40.

39 Verify wiring from DTE device to Craft 2 port per DLP-553 and Figure 2; then go to step 43.

40 Verify wiring from modem to Craft 2 port per DLP-553 and Figure 2.

41 ***NOTE:*** *The Craft 2 interface requires an odd numbered COA plug-in unit, (i.e., COA601, COA603, etc.)*

Is an odd numbered COA installed?

If yes, go to step 48.
If no, go to step 42.

42 **CAUTION: Possibility of service interruption. Verify that there are no system alarms before replacing COA.**

43 Replace COA with an odd numbered COA [DLP-101].

44 Add new COA to database [DLP-549].

45 If necessary, unassign the SE2A port if it is entered in-service [DLP-501].

46 If necessary, place Craft 2 port in-service [DLP-502].

47 STOP. This procedure is complete.

48 Go to the NE and log on using the Craft 1 port [DLP-117].

49 Retrieve provisioned parameters for ports [DLP-502].

50 Analyze the provisioning of port parameters (refer to Table B) and verify that the port is entered into service (Primary State is not OOS-MA-UAS).

51 Is Primary State of port = OOS-MA-UAS?

If yes, go to step 52.
If no, go to step 54.

52 Enter Craft 2 port in-service [DLP-502].

53 STOP. This procedure is complete.

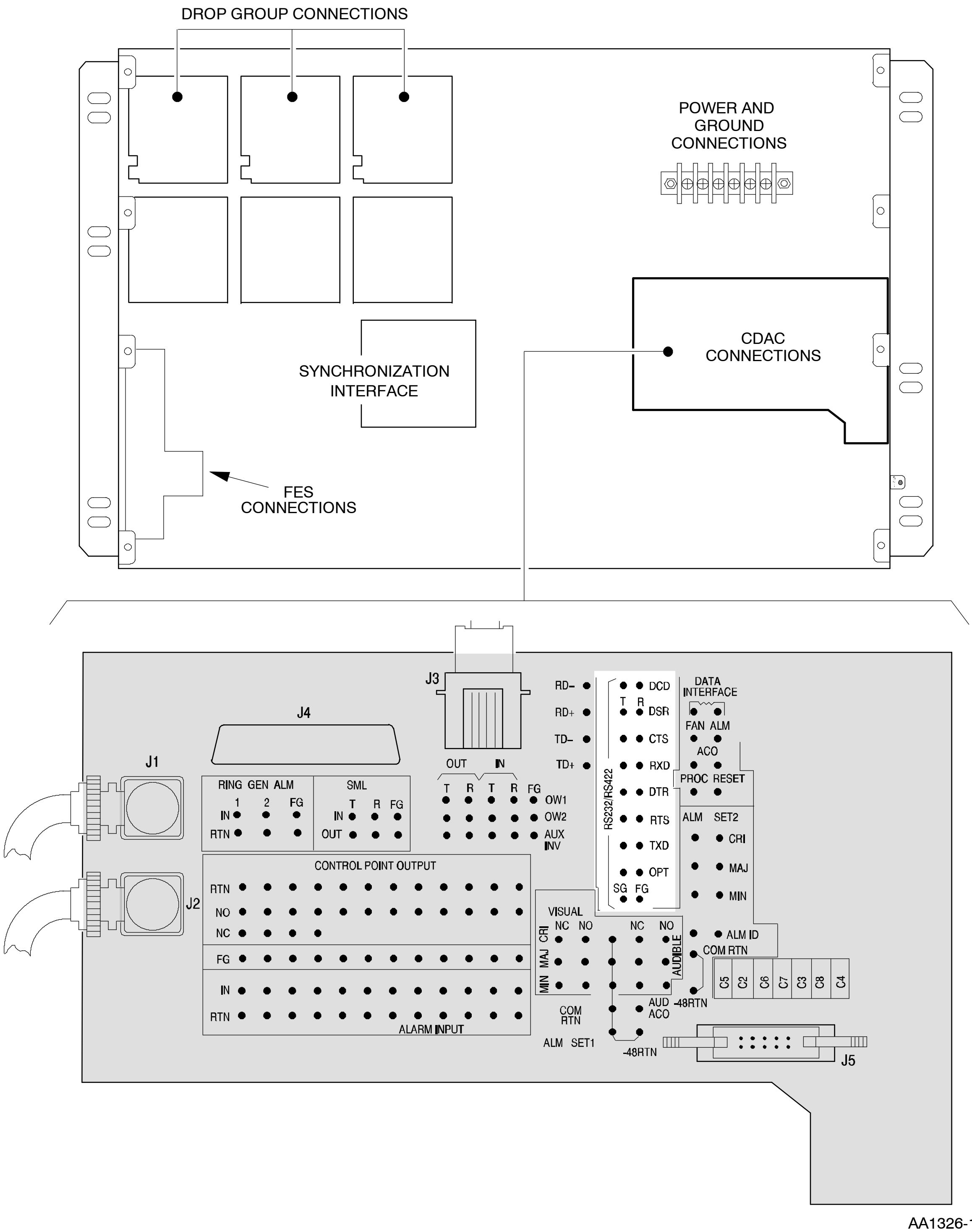


Figure 2. 1603 SMX Rear View

54 Retrieve Craft 2 port provisioned parameters [DLP-502] and compare those parameters to the PC communications port settings.

55 Are the Craft 2 port parameter settings and the PC communications port settings compatible?

If no, go to step 56.
If yes, go to step 60.

56 Do you need to modify port parameter settings or PC communications port settings?

If PC settings, go to step 57.
If port parameter settings, go to step 58.

57 Change parameters for PC terminal emulator being used (refer to Tables C and D); then go to step 59.

58 Modify the required Craft 2 port parameters [DLP-502].

59 Is communication with NE established?

If yes, STOP. This procedure is complete.
If no, go to step 60.

60 Suspect a faulty COA or NEP plug-in unit. Go to TAP-021.

61 STOP. This procedure is complete.

TAP-041
Clear Far-End Alarm (Lighted REM ALM LED on COA)

Purpose

Provides procedures for clearing a far-end alarm.

STEP	PROCEDURE
1	**NOTE:** *The REM ALM LED indicates that a far-end alarm exists at one of the NEs in the network.*
2	See Figure 1 for location of COAxxx plug-in (COA).
3	On COA, press and hold the ID SEL button. **NOTE:** *Network Element identification (NE ID) numbers (1...32) are listed, one at a time, on the two seven-segment displays for about three seconds each. If any alarms are present at the NE being listed, the associated alarm severity LEDs (CRI, MJ, and MN) also light.*
4	Note alarm severity for each NE ID.
5	Release the ID SEL button after all NE IDs have been listed. After about five seconds, the NE ID display goes blank.
6	From office records, determine which NE the NE ID corresponds to, or log on to the FEALM concentrator [DLP-117], and retrieve RADMAP concentrator information [DLP-562].
7	Either go to the alarmed NE or remotely log on to the NE [DLP-117] and resolve the alarms [IXL-001].
8	STOP. This procedure is complete.

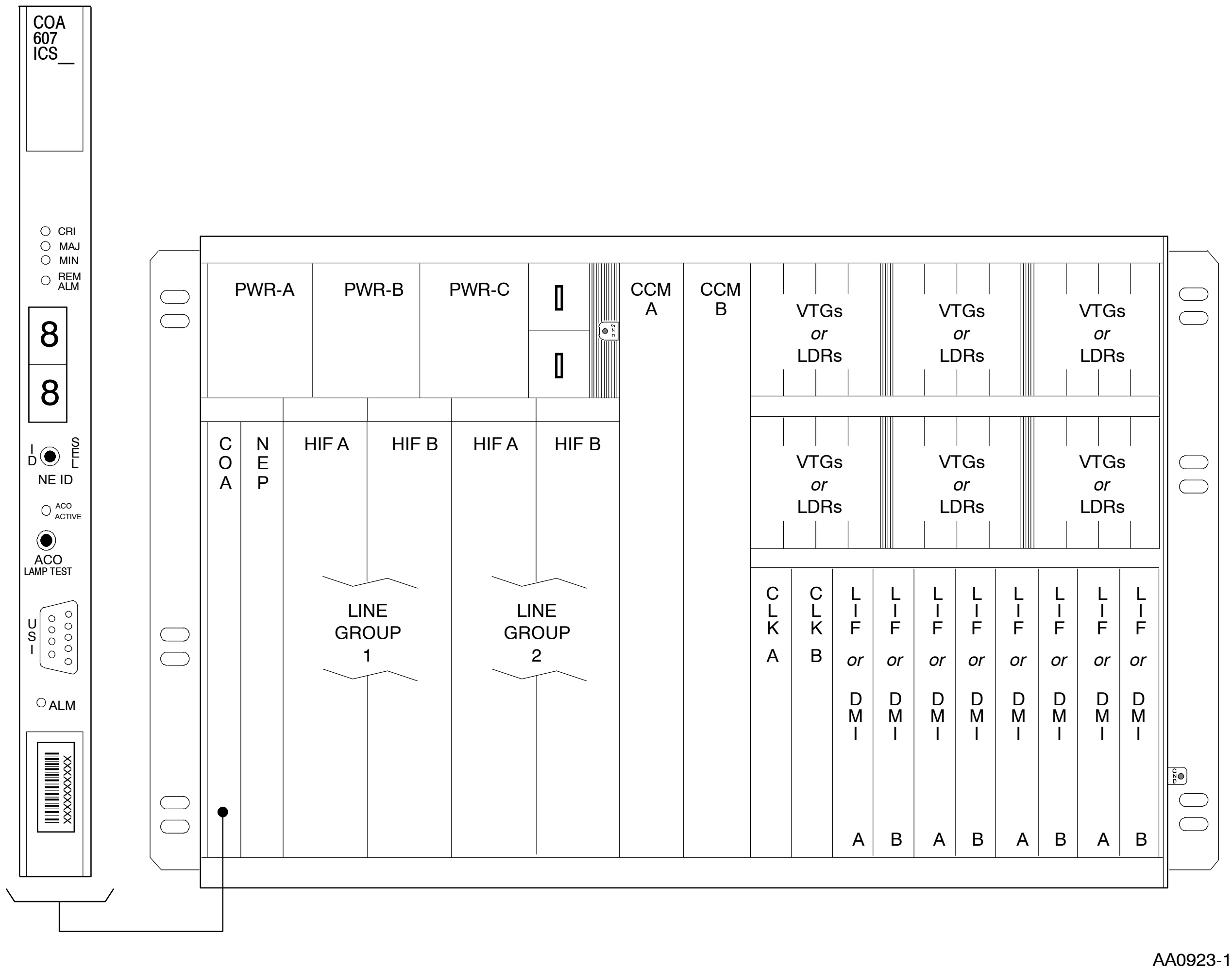


Figure 1. COAxxx Plug-in Unit

TAP-043
Clear T3 (DS3) Alarm

Purpose

Provides procedures for clearing T3 (DS3) alarms.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Retrieve alarms at local NE [DLP-100].
2	Are there any LIF or LDR alarm indications on drop group with alarmed DS3? If yes, go to TAP-021 to resolve. If no, go to step 3.
3	Is far-end terminal a 1603 SM or 1603 SMX network element? If yes, go to step 5. If no, go to step 4.
4	Go to far-end terminal and check for alarms using other vendor's documentation. If no problems are found, go to step 7.
5	Retrieve alarms at far-end [DLP-100].
6	Are any alarms being reported at the far-end NE? If yes, clear these alarms. Refer to TAP-001. If no, go to step 7.
7	Have DS3 alarms and conditions been retrieved? If yes, go to step 9. If no, go to step 8.
8	Retrieve DS3 alarms [DLP-100].
9	Identify the condition; then go to the step indicated in Table A to clear alarm.

Table A. T3 Facility Alarms/Conditions/Events

ALARM/ CONDITION	REASON FOR ALARM	STEP
AIS	Alarm indication signal detected (NEND RCV)	10
	Alarm indication signal detected (NEND TRMT)	10
BERL-HT	Bit Error Ratio Line-High Threshold. The T3 facility has detected that the number of bits in error to the number of bits transmitted has degraded to the point of exceeding a set threshold, 10^{-4} to 10^{-9}. Signal failure is imminent.	15
FRMMF	Frame Format Mismatch Failure. A mismatch has been detected on the DS3 facility (RCV NEND). The detection of C-Bit framing format while in M23 mode or vice versa is a typical cause of this alarm.	101
ISD	Receive Idle Signal Detected. A normal signal source is not present, (i.e., a fixed-pattern coded signal has been placed on the output from the far end because no payload is assigned to that channel). The idle signal has a valid M-Frame alignment channel, M-subframe alignment channel, and P-Bit channel, but no payload.	109
INHLPBK	Inhibit Loopback	114
INHPMREPT	Inhibit PM reports	116
LOF	Loss of Frame. LOF has been detected at the local NE in the demux direction from the SONET network. (NEND TRMT). Any of the following conditions could cause this alarm: end-to-end mismatch of frame-format provisioning; LOF on remote facility; Line Buildout (LBO) at remote LTE; failure of LIF or LDR plug-in on either end; or network problems (incorrect cross-connect, etc.).	120
	Loss of Frame has been detected at the local NE in the mux direction from the DS3 facility. (NEND RCV)	127
LOS	Loss of Signal (NEND RCV). An LOS could be caused by one of the following: a loss of a receive signal; an all zeros pattern for over 100 msec; or loss of clock recovery.	134
MTCE	Removed from service for maintenance	141
RAI	Remote Alarm Indication. Failures such as LOS, LOF, and AIS at the far end result in the transmission of a continuous RAI signal in the reverse direction (i.e., toward the near-end NE). The RAI signal is carried by the Far-End Alarm and Control (FEAC) channel.	143

Table A. T3 Facility Alarms/Conditions/Events (cont)

ALARM/ CONDITION	REASON FOR ALARM	STEP
RAIXBIT	Remote Alarm Indication (XBIT). Failures at the far end result in the transmission of a continuous RAIXBIT signal in the reverse direction (i.e., toward the near-end NE) via the X-Bit channel. These failures include: an equipment failure that is DS3 service affecting, LOS, LOF and AIS.	143
T-BPV	Bipolar violations TCA* (NEND RCV)	146
T-CVCPP	CP-Parity errors - Path TCA* (NEND RCV)	146
	CP-Parity errors - Path TCA* (NEND TRMT)	146
	CP-Parity errors - Path TCA* (FEND RCV)	146
T-CVL	Coding violations TCA* (NEND RCV)	146
T-CVPP	P-parity errors - Path TCA* (NEND RCV)	146
	P-parity errors - Path TCA* (NEND TRMT)	146
T-ESCPP	CP-Bit errored seconds - Path TCA* (NEND RCV)	146
	CP-Bit errored seconds - Path TCA* (NEND TRMT)	146
	CP-Bit errored seconds - Path TCA* (FEND RCV)	146
T-ESL	Errored seconds - Line TCA* (NEND RCV)	146
T-ESPP	P-Bit errored seconds - Path TCA* (NEND RCV)	146
	P-Bit errored seconds - Path TCA* (NEND TRMT)	146
T-SASCP	X-bits seconds -Path TCA* (FEND RCV)	146
T-SASP	SEF/AIS seconds - Path TCA* (NEND RCV)	146
	SEF/AIS seconds - Path TCA* (NEND TRMT)	146
T-SESCPP	CP-Bit sev. errored secs. - Path TCA* (NEND RCV)	146
	CP-Bit sev. errored secs. - Path TCA* (NEND TRMT)	146
	CP-Bit sev. errored secs. - Path TCA* (FEND RCV)	146
T-SESL	Severely errored seconds - Line TCA* (NEND RCV)	146
T-SESPP	P-Bit sev. errored secs. - Path TCA* (NEND RCV)	146
	P-Bit sev. errored secs. - Path TCA* (NEND TRMT)	146
T-UASCPP	CP-Bit unavailable seconds - Path TCA* (NEND RCV)	146
	CP-Bit unavailable seconds - Path TCA* (NEND TRMT)	146
	CP-Bit unavailable seconds - Path TCA* (FEND RCV)	146
T-UASPP	P-Bit unavailable seconds - Path TCA* (NEND RCV)	146
	P-Bit unavailable seconds - Path TCA* (NEND TRMT)	146

Table A. T3 Facility Alarms/Conditions/Events (cont)

CONDITION	DESCRIPTION	ACTION
ACTLPBK	Loopback is active (Loopback type, location, request types are displayed as comment)	No Action
AINS	Automatic-In-Service state	No Action
CONNTESTACT	Test T3 is connected (Pattern = IDLE or QRSS are displayed as comment)	No Action
FEAC-( )	Far-end alarm and control code received - (character representation of FEAC code is displayed as comment): DS3EQPT-SA, DS3LOS, DS3OOF, DS3AIS, DS3IDLE, DS3EQPT-NSA, COMMEQPT-NSA, MDS1LOS, DS1EQPT-SA, DS1LOS, DS1EQPT-NSA, or UNDEFINED	No Action
DS3AIS	DS3 AIS received (DS3 AIS type is displayed as comment): 0101 with stuck stuffing 0101 without stuck stuffing 1010 with stuck stuffing (NAS) 1010 without stuck stuffing (BLUE)	No Action
QRSS	Quasi-random pattern is detected on RCV facility	No Action
Event	**Description**	**Action**
ACTLPBK	Loopback is active	No Action
AINS	Automatic-In-Service state	No Action
IS-AUTO	Automatic OOS-MA to IS	No Action
* *TCA = Threshold Crossing Alert*		

Alarm/Condition – AIS

10 Is direction of AIS alarm RCV (receive) or TRMT (transmit)?

If RCV, go to step 11.
If TRMT, Go to step 13.

11 Troubleshoot far-end equipment. AIS is received on incoming (input, mux direction) DS3 facility.

12 STOP. This procedure is complete.

13 Troubleshoot far-end NE where DS3 facility enters SONET network. AIS is received on incoming signal (input, demux direction) from SONET network.

14 STOP. This procedure is complete.

Alarm/Condition – BERL-HT

15 Check coax cable connections at 1603 SMX backplane and cross-connection panel. Correct connections, if necessary.

16 If connections are correct, retrieve Line Buildout parameters at far-end NE (if NE is a 1603 SMX, 1603 SM, or 1603 SE) [DLP-525].

17 From the response, verify that provisioning of Line Buildout parameter agrees with office records. Refer to Table B for recommended setting based on cable types.

Table B. Line Buildout Settings

TYPE AND DISTANCE OF CABLE	DISTANCE (FEET)	SETTING*
AT&T 728A or equivalent cable	0–225	Yes
AT&T 728A or equivalent cable	226–450	No
AT&T 734A or equivalent cable	0–200	Yes
AT&T 734A or equivalent cable	201–400	No
AT&T 735A or equivalent cable	0–110	Yes
AT&T 735A or equivalent cable	111–220	No

* *The Line Buildout setting (Yes or No) depends on the type of coax cable used and the distance to the DS3 cross-connect.*

18 Does Line Buildout parameter need to be changed?

If yes, go to step 19.
If no, go to step 21.

19 Change Line Buildout parameter at the far-end NE [DLP-525]; then retrieve alarms [DLP-100].

20 Did BERL-HT alarm clear (may take several minutes to clear)?

If yes, STOP. This procedure is complete.
If no, go to step 21.

21 Identify the type of LIF carrying the alarmed DS3 facility; then go to the step indicated in Table C to test LIF and LDR that are carrying the alarmed facility.

22 **CAUTION: Possibility of service interruption. Adhere to the procedure in DLP-101 when replacing an LIF or LDR to avoid service interruption.**

Table C. Types of LIFs

IF DROP GROUP IS EQUIPPED WITH AN...	AND UNIT IS...	THEN GO TO...
LIF201	Non-redundant	Step 23
	Redundant	Step 39
LIF501701	Non-redundant	Step 23
	Redundant	Step 61
LIFD01	Non-redundant	Step 72
	Redundant	Step 88

Test Non-redundant LIF201 or LIF501/701 Unit

23 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF and LDR units. If DS3 facility is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

24 Place LIF to be diagnosed in maintenance state (OOS-MT-MAN) [DLP-501].

25 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

26 Did diagnostics pass?

If yes, go to step 29.
If no, go to step 27.

27 Replace LIF per DLP-101.

28 STOP. This procedure is complete.

29 Place LIF back in-service [DLP-501].

30 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR.**

31 Place LDR to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

32 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

33 Did diagnostics pass?

If yes, problem must be at far-end terminal. Go to step 36.
If no, go to step 34.

34 Replace LDR per DLP-101.

35 STOP. This procedure is complete.

36 Place LDR back in-service [DLP-501]; then analyze and clear alarms at far-end NE.

37 If BERL-HT alarm persists, test coax facility per local procedure or contact Customer Service.

38 STOP. This procedure is complete.

Test Redundant LIF201 Unit

NOTE: *The active and standby LIFs will be switched to determine whether the active LIF or active LDR is causing the BERL-HT alarm.*

39 Switch to redundant LIF [DLP-505].

NOTE: *When LIF20x units are switched, the LDRs also switch, (i.e., LDR-A is active when LIF-A is active, and LDR-B is active when LIF-B is active).*

40 Retrieve alarms [DLP-100].

41 Did BERL-HT alarm clear (may take several minutes)?

If yes, problem must be in standby LIF or LDR. Go to step 45.
If no, problem must be at far-end terminal. Go to step 42.

42 Analyze and clear alarms at far-end NE.

43 If BERL-HT alarm persists, test coax facility per local procedure or contact Customer Service.

44 STOP. This procedure is complete.

45 **CAUTION: Possibility of service interruption. Diagnostics are service-affecting if performed on active units. Be sure the LIF and LDR units are in standby before performing diagnostics.**

46 Place LIF to be diagnosed in maintenance state (OOS-MT-MAN) [DLP-501].

47 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

48 Did diagnostics pass?

If yes, go to step 51.
If no, go to step 49.

49 Replace LIF per DLP-101.

50 STOP. This procedure is complete.

51 Place LIF back in-service [DLP-501].

52 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR. Be sure the LIF and LDR units are in standby before performing diagnostics.**

53 Place LDR to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

54 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

55 Did diagnostics pass?

If yes, problem must be at far-end terminal. Go to step 58.
If no, go to step 56.

56 Replace LDR per DLP-101.

57 STOP. This procedure is complete.

58 Place LDR back in-service [DLP-501]; then analyze and clear alarms at far-end NE.

59 If BERL-HT alarm persists, test coax facility per local procedure or contact Customer Service.

60 STOP. This procedure is complete.

Test Redundant LIF501/701 Unit

NOTE: *The active and standby LIFs associated with the alarmed facility will be switched to determine whether the active LIF is causing the BERL-HT alarm. If the BERL-HT alarm isn't cleared, the active and standby LDRs associated with the alarmed facility will be switched.*

61 Switch to redundant LIF [DLP-505]; then retrieve alarms [DLP-100].

62 Did BERL-HT alarm clear (may take several minutes)?

If yes, go to step 63.
If no, go to step 65.

63 Replace standby LIF per DLP-101.

64 STOP. This procedure is complete.

65 Switch to redundant LDR [DLP-505]; then retrieve alarms [DLP-100].

66 Did BERL-HT alarm clear (may take several minutes)?

If yes, go to step 67.
If no, problem must be at far-end terminal. Go to step 69.

67 Replace standby LDR per DLP-101.

68 STOP. This procedure is complete.

69 Analyze and clear alarms at far-end NE.

70 If BERL-HT alarm persists, test coax facility per local procedure or contact Customer Service.

71 STOP. This procedure is complete.

Test Non-redundant LIFD01 Unit

NOTE: *Diagnostics will be performed on the LIF associated with the alarmed facility. If diagnostics pass, the protection LDR and the LDR associated with the alarmed facility will be switched.*

72 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF unit. If DS3 facility is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

73 Place LIF to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

74 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

75 Did diagnostics pass?

If yes, go to step 78.
If no, go to step 76.

76 Replace LIF per DLP-101.

77 STOP. This procedure is complete.

78 Place LIF back in-service [DLP-501].

79 Identify the LDR that is carrying the alarmed DS3 facility [DLP-565] and switch that LDR to protection [DLP-529].

NOTE: *Revertive switch may occur. Inhibit switch back to working if required.*

80 Wait several minutes; then retrieve alarms [DLP-100].

81 Did BERL-HT alarm clear?

If yes, then go to step 82.
If no, problem must be at far-end terminal. Go to step 84.

82 Identify the physical location of the LDR that was switched to protection [DLP-565] and replace that LDR per DLP-101.

83 STOP. This procedure is complete.

84 Analyze and clear alarms at far-end NE.

85 If BERL-HT alarm persists, test coax facility per local procedure or contact Customer Service.

86 If switch back to working was inhibited, allow automatic switching to working unit [DLP-536].

87 STOP. This procedure is complete.

Test Redundant LIFD01 Unit

NOTE: *The active and standby LIFs associated with the alarmed facility will be switched to determine whether the active LIF is causing the BERL-HT alarm. If the BERL-HT alarm isn't cleared, the protection LDR and the LDR associated with the alarmed facility will be switched.*

88 Switch to redundant LIF [DLP-505]; then retrieve alarms [DLP-100].

89 Did BERL-HT alarm clear (may take several minutes)?

If yes, go to step 90.
If no, go to step 92.

90 Replace standby LIF per DLP-101.

91 STOP. This procedure is complete.

92 Identify the LDR that is carrying the alarmed DS3 facility [DLP-565] and switch that LDR to protection [DLP-529].

NOTE: *Revertive switch may occur. Inhibit switch back to working if required.*

93 Wait several minutes; then retrieve alarms [DLP-100].

94 Did BERL-HT alarm clear?

If yes, then go to step 95.
If no, problem must be at far-end terminal. Go to step 97.

95 Identify the physical location ot the LDR that was switched to protection [DLP-565] and replace that LDR per DLP-101.

96 STOP. This procedure is complete.

97 If switch back to working was inhibited, allow automatic switching to working unit [DLP-536].

98 Analyze and clear alarms at far-end NE.

99 If BERL-HT alarm persists, test coax facility per local procedure or contact Customer Service.

100 STOP. This procedure is complete.

Alarm/Condition – FRMMF (LIF601 DS3/DS1 Transmux Only)

101 Retrieve DS3 facility parameters [DLP-502].

102 Is DS3 Format parameter provisioned correctly per office records?

If yes, go to step 105.
If no, go to step 103.

103 Change provisioning of the DS3 Format parameter [DLP-502].

104 STOP. This procedure is complete.

105 Check far-end equipment for frame format type; correct if necessary.

106 Check facility wiring and connections; correct if necessary.

107 Was source of FRMMF alarm found and cleared?

If yes, STOP. This procedure is complete.
If no, go to step 21 to test LIF and LDR.

108 STOP. This procedure is complete.

Alarm/Condition – ISD (LIF601 DS3/DS1 Transmux Only)

109 Is DS3 facility generating alarm carrying traffic?

If yes, go to step 111.
If no, ignore alarm.

110 STOP. This procedure is complete.

111 Check far end to determine if/why fixed pattern condition is being generated.

112 If alarm persists, troubleshoot DS3 facilities.

113 STOP. This procedure is complete.

Alarm/Condition – INHPMREPT

114 To clear alarm, allow PM reporting on DS3 facility [DLP-510].

115 STOP. This procedure is complete.

Alarm/Condition – INHLPBK (LIF601 DS3/DS1 Transmux Only)

116 To clear alarm, allow remote activation of loopbacks on DS3 facility [DLP-548].

117 STOP. This procedure is complete.

Alarm/Condition – LOF

118 Retrieve alarms and determine Direction of LOF alarm [DLP-100].

119 What is the direction of LOF alarm?

If Transmit, go to step 120.
If Receive (or blank), go to step 127.

LOF – NEND, TRMT Direction

120 Verify that the DS3 Format parameter is provisioned the same at local NE and remote NE [DLP-519] and also at remote LTE (use vendor's documentation).

121 Is DS3 Format parameter provisioned the same at these three locations?

If yes, go to step 124.
If no, go to step 122.

122 Determine correct DS3 Format parameter setting from office records and reprovision the incorrect DS3 port [DLP-519].

NOTE: *LIF601 only supports C-BIT and M23 formats.*

123 STOP. This procedure is complete.

124 **NOTE:** *Line buildout is applied in the transmit direction. An incorrect LBO setting at the remote LTE may cause LOF at the remote NE (RCV direction) and local (alarmed) NE (TRMT direction).*

Check LBO at remote LTE per vendor's documentation. Correct if necessary.

125 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 21 and test LIF and LDR.

126 STOP. This procedure is complete.

LOF – NEND, RCV Direction

127 Verify the DS3 Format parameter is provisioned the same at the local NE [DLP-519] and local LTE (use vendor's documentation) .

128 Is DS3 Format parameter provisioned the same at local NE and local LTE?

If yes, go to step 131.
If no, go to step 129.

129 Determine correct DS3 Format parameter setting from office records, and reprovision the incorrect DS3 port [DLP-519].

NOTE: *LIF601 only supports C-BIT and M23 formats.*

130 STOP. This procedure is complete.

131 ***NOTE:*** *Line buildout is applied in the transmit direction. An incorrect LBO setting at the local LTE may cause LOF at the local NE (RCV direction) and remote NE (TRMT direction).*

Check LBO at local LTE per vendor's documentation; correct if necessary.

132 Did the alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 21 and test LIF and LDR.

133 STOP. This procedure is complete.

Alarm/Condition – LOS

134 Check coax cable connections at 1603 SMX backplane and cross-connection panel. Correct connections, if necessary.

135 From office records, determine how the DS3 Line Buildout parameter should be provisioned at the far-end terminal.

136 Retrieve DS3 facility parameters at the far-end terminal and note provisioned value of Line Buildout parameter [DLP-525].

137 Does provisioned value of Line Buildout parameter agree with office records?

If yes, then go to step 21 and test LIF and LDR.
If no, then go to step 138.

138 Change parameter to agree with office records [DLP-525].

139 Did alarm clear (may take several minutes to clear)?

If yes, then go to step 140.
If no, go to step 21 and test LIF and LDR.

140 STOP. This procedure is complete.

Alarm/Condition – MTCE

141 To clear alarm, change service state to in-service [DLP-501].

142 STOP. This procedure is complete.

Alarm/Condition – RAI/RAIXBIT (LIF601 DS3/DS1 Transmux Only)

143 ***NOTE:*** *RAI and RAIXBIT replace yellow alarms. RAIXBIT is only applicable to M23 format.*

At the far-end, check for an equipment failure that is DS3 service-affecting. Also check for LOS, LOF and AIS alarms. Troubleshoot, if present.

144 Did alarm clear (may take several minutes to clear)?

If yes, STOP. This procedure is complete.
If no, go to step 21 and test LIF and LDR.

145 STOP. This procedure is complete.

Alarm/Condition – T-xxx

NOTE: *A threshold crossover alarm has been generated because one of the performance parameters exceeds the value specified for it (refer to Table D).*

Table D. DS3 PM Thresholds

MONITOR TYPE	FACTORY DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERL-HT	4		4...9	Bit Error Ratio Line – High Threshold
BPV	387	3865	1...4,294,967,295	Bipolar Violations
CVCPP	382	3820	1...4,294,967,295	CP-Bit errors
CVL	387	3865	1...4,294,967,295	Line coding errors
CVPP	382	3820	1...4,294,967,295	P-Bit errors
DSESCPP	44		1...65535	SESCPP coding violations
DSESL	44		1...65535	Number of coding violations to make one SESL
DSESPP	44		1...65535	SESPP coding violations
ESCPP	25	250	1...65535	CP-Bit path errored seconds
ESL	25	250	1...65535	Line Errored Seconds
ESPP	25	250	1...65535	P-Bit path errored seconds
SASP	2	8	1...65535	SEF/AIS seconds

Table D. DS3 PM Thresholds (cont)

MONITOR TYPE	FACTORY DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
SASCP	2	8	1...65535	SEF/AIS (X-Bits)
SESCPP	4	40	1...65535	CP-Bit path SES
SESL	4	40	1...65535	Line Severely Errored Seconds
SESPP	4	40	1...65535	P-Bit path SES
UASCPP	10	10	1...65535	CP-Bit path unavailable seconds
UASPP	10	10	1...65535	P-Bit path unavailable seconds

146 Retrieve current conditions for DS3 facility [DLP-100].

147 Are there any other facility alarms (besides T-xxx)?

If yes, go to step 148.
If no, go to step 150.

148 Correct facility alarms before resolving TCA conditions per Table A.

149 STOP. This procedure is complete.

150 Is the condition severe enough to warrant unit replacement?

If yes, go to step 153.
If no, go to step 151.

151 Record the alarm as an event.

152 STOP. This procedure is complete.

153 From the Retrieve Conditions work view opened in step 146, determine Location and Direction of T-xxx condition. (See Figure 1 for definition of Location and Direction parameters.)

154 What is Location and Direction of T-xxx condition?

If Near End and Receive (or blank), go to step 155.
If Near End and Transmit, go to step 156.
If Far End and Receive (or blank), go to step 157.

155 Check for problems in the local DS3 facility or LTE. Clear any problems that are found then go to step 158.

156 Look for other alarms in the SONET network between the local and remote NEs. Refer to TAP-001.

157 Check for problems in the local DS3 facility or the local NE. Clear any problems that are found then go to step 158.

158 Was problem found and corrected in facility?

If yes, STOP. This procedure is complete.
If no, go to step 159.

159 Are Line or Path errors present?

If Line, go to step 164.
If Path, go to step 160.

160 For path T–xxx conditions only, check provisioning of DS3 Frame Format parameter at local NE [DLP-519].

161 Is Frame Format parameter correct for signal or facility?

If yes, go to step 164.
If no, go to step 162.

162 Determine correct format parameter from office records and if necessary reprovision the incorrect DS3 port [DLP-519].

NOTE: *LIF30x only supports Clear Channel format. LIF601 only supports C-BIT and M23 formats.*

163 STOP. This procedure is complete.

164 **NOTE:** *The far end is detecting a problem on the receive (facility) side. Problem is most likely at near-end equipment or on the facility.*

Identify the type of LIF carrying the alarmed DS3 facility; then go to the step indicated in Table E to test LIF and LDR that are carrying the alarmed facility.

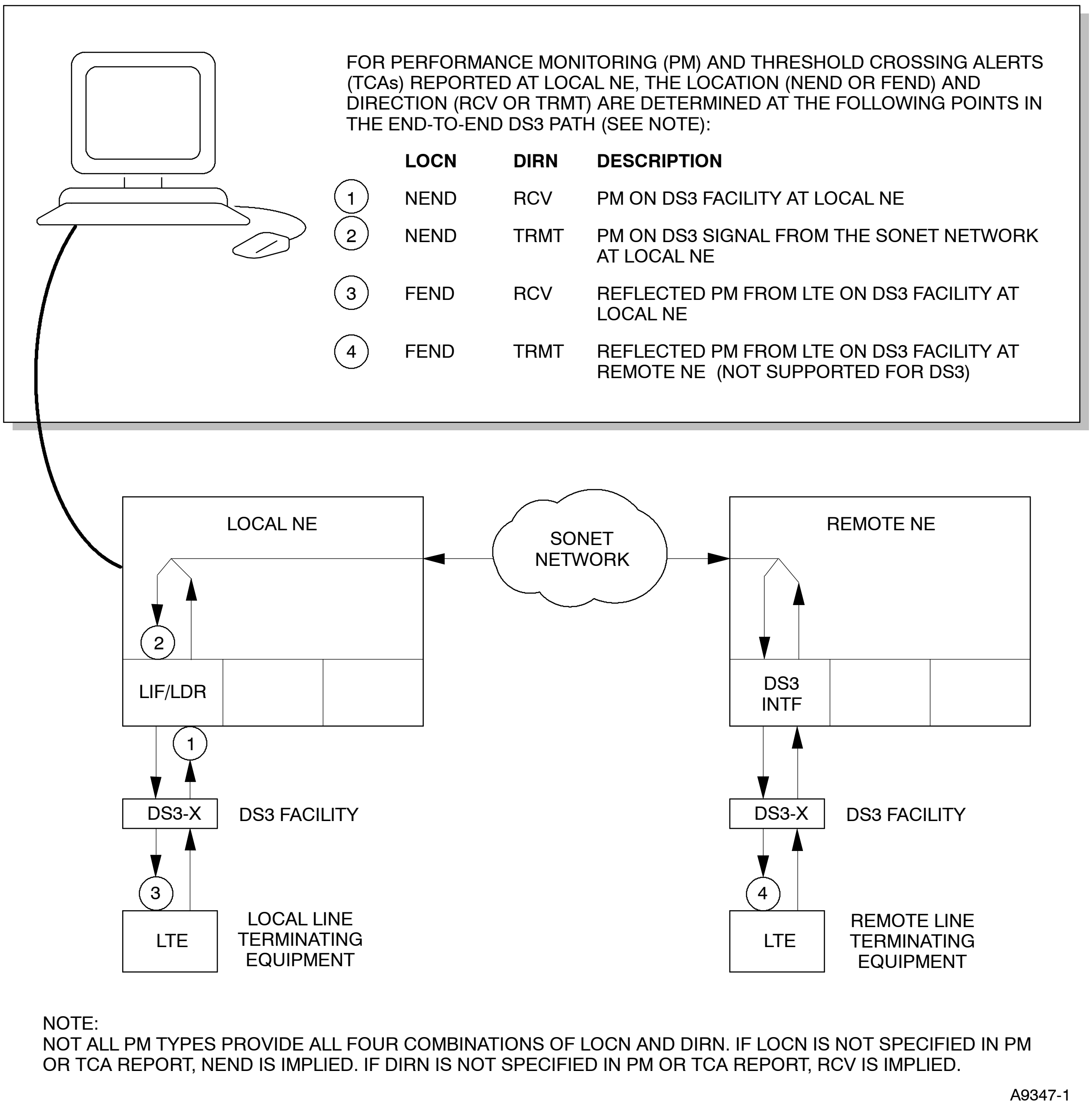


Figure 1. PM Monitoring Points in DS3 Circuit

Table E. Types of LIFs

IF DROP GROUP IS EQUIPPED WITH AN...	AND UNIT IS...	THEN GO TO...
LIF201	Non-redundant	Step 165
	Redundant	Step 180
LIF501/701	Non-redundant	Step 165
	Redundant	Step 201
LIFD01	Non-redundant	Step 213
	Redundant	Step 226

Test Non-redundant LIF201 or LIF501/701 Unit

165 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF and LDR units. If facility is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

166 At the near-end NE, place LIF to be diagnosed in maintenance state (OOS-MT-MAN) [DLP-501].

167 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

168 Did diagnostics pass?

If yes, go to step 171.
If no, go to step 169.

169 Replace LIF per DLP-101.

170 STOP. This procedure is complete.

171 Place LIF back in-service [DLP-501].

172 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR.**

173 Place LDR to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

174 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

175 Did diagnostics pass?

If yes, problem is most likely in facility. Go to step 178.
If no, go to step 176.

176 Replace LDR per DLP-101.

177 STOP. This procedure is complete.

178 Place LDR back in-service [DLP-501]; then troubleshoot facility per local practice.

179 STOP. This procedure is complete.

Test Redundant LIF201 Unit

NOTE: *The active and standby LIFs will be switched to determine whether the active LIF or active LDR is causing the alarm.*

180 Switch to redundant LIF [DLP-505].

NOTE: *When LIF20x units are switched, the LDRs also switch, (i.e., LDR-A is active when LIF-A is active, and LDR-B is active when LIF-B is active).*

181 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

182 Did PM errors stop?

If yes, problem must be in standby LIF or LDR. Go step 185.
If no, problem is most likely in the facility. Go to step 183.

183 Troubleshoot facility per local practice.

184 STOP. This procedure is complete.

185 **CAUTION: Possibility of service interruption. Diagnostics are service-affecting if performed on active units. Be sure the LIF and LDR units are in standby before performing diagnostics.**

186 Place LIF to be diagnosed in maintenance state (OOS-MT-MAN) [DLP-501].

187 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

188 Did diagnostics pass?

If yes, go to step 191.
If no, go to step 189.

189 Replace LIF per DLP-101.

190 STOP. This procedure is complete.

191 Place LIF back in-service [DLP-501].

192 **CAUTION: Possibility of service interruption. The following steps are service-affecting if performed on the active LDR. Be sure the LIF and LDR units are in standby before performing diagnostics.**

193 Place LDR to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

194 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

195 Did diagnostics pass?

If yes, problem most likely in facility. Go to step 198.
If no, go to step 196.

196 Replace LDR per DLP-101.

197 STOP. This procedure is complete.

198 Place LDR back in-service [DLP-501]; then troubleshoot facility per local practice.

199 STOP. This procedure is complete.

Test Redundant LIF501/701 Unit

NOTE: *The active and standby LIFs associated with the alarmed facility will be switched to determine whether the active LIF is causing the alarm. If the alarm isn't cleared, the active and standby LDRs associated with the alarmed facility will be switched.*

200 **CAUTION: Possibility of service interruption when replacing an LIF or LDR unit. Adhere to the procedure in DLP-101 when replacing these units to avoid service interruption.**

201 Switch to redundant LIF [DLP-505].

202 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

203 Did PM errors stop?

If yes, go to step 204.
If no, go to step 206.

204 Replace standby LIF per DLP-101.

205 STOP. This procedure is complete.

206 Switch to redundant LDR [DLP-505].

207 Wait several minutes; then retrieve PM registers [DLP-517].

208 Did PM errors stop?

If yes, go step 209.
If no, problem most likely in facility. Go to step 211.

209 Replace standby LDR per DLP-101.

210 STOP. This procedure is complete.

211 Troubleshoot facility per local practice.

212 STOP. This procedure is complete.

Test Non-redundant LIFD01 Unit

NOTE: *Diagnostics will be performed on the LIF associated with the alarmed facility. If diagnostics pass, the protection LDR and the LDR associated with the alarmed facility will be switched.*

213 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF unit. If facility is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

214 Place LIF to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

215 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

216 Did diagnostics pass?

If yes, place LIF back in-service [DLP-501; then go to step 218.
If no, replace LIF per DLP-101.

217 STOP. This procedure is complete.

218 Identify the LDR501 that is carrying the alarmed DS3 facility [DLP-565] and switch that LDR to protection [DLP-529].

NOTE: *Revertive switch may occur. Inhibit switch back to working if required.*

219 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

220 Did PM errors stop?

If yes, go step 221.
If no, go to step 223.

221 Identify the physical location of the LDR501 that was switched to protection [DLP-565] and replace that LDR per DLP-101.

222 STOP. This procedure is complete.

223 If switch back to working was inhibited, allow automatic switching to working unit [DLP-536].

224 Problem is most likely in facility. Troubleshoot per local practice.

225 STOP. This procedure is complete.

Test Redundant LIFD01 Unit

NOTE: *The active and standby LIFs associated with the alarmed facility will be switched to determine whether the active LIF is causing the alarm. If the alarm isn't cleared, the protection LDR and the LDR associated with the alarmed facility will be switched.*

226 Switch to redundant LIF [DLP-505].

227 Wait several minutes; then retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

228 Did PM errors stop?

If yes, go step 229.
If no, go to step 231.

229 Replace standby LIF per DLP-101.

230 STOP. This procedure is complete.

231 Identify the LDR501 that is carrying the alarmed facility [DLP-565] and switch that LDR to protection [DLP-529].

NOTE: *Revertive switch may occur. Inhibit switch back to working if required.*

232 Wait several minutes; then retrieve PM registers [DLP-517].

233 Did PM errors stop?

If yes, go step 234.
If no, go to step 236.

234 Identify the physical location of the LDR that was switched to protection [DLP-565] and replace that LDR per DLP-101.

235 STOP. This procedure is complete.

236 If switch back to working was inhibited, allow automatic switching to working unit [DLP-536].

237 Problem most likely in facility. Troubleshoot per local practice.

238 STOP. This procedure is complete.

TAP-044
Clear LAN Alarm

Purpose

Provides procedures for clearing LAN alarms.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

STEP	PROCEDURE
1	Retrieve LAN protocol provisioning data [DLP-502] and check the data link layer provisioning for the External Domain selection. (It should be set to N.)
2	Check LAN Type to verify it is correct setting for the LAN Type (10Base2 or 10BaseT).
3	Were errors found in LAN provisioning? If yes, go to step 4. If no, go to step 6.
4	Correct LAN protocol provisioning errors [DLP-502].
5	STOP. This procedure is complete.
6	Retrieve alarms [DLP-100].
7	On the Alarms work view, determine which LAN condition is producing the alarm.
8	Select alarm condition type (condlan in step 7); refer to Table A.

Table A. Alarms/Events

ALARM/CONDITION	REASON FOR ALARM	GO TO STEP...
CARLOS	Loss of carrier was encountered by the LAN controller during frame transmission. This alarm is sent once and does not clear until either a good transmission occurs or a good frame is received.	9
DUPADR	The LAN initialization duplicate address check found a duplicate address.	18
Event	**Description**	**Action**
EXCOL	Excessive collisions	No action

Alarm/Condition – CARLOS

9 Has provisioning been eliminated as an alarm cause?

If yes, go to step 10.
If no, return to step 1.

10 Check LAN wiring [DLP-020].

11 Was LAN wiring correct?

If yes, go to step 13.
If no, correct per DLP-020.

12 STOP. This procedure is complete.

13 ***NOTE:*** *LAN port must be in-service (IS) for data packets to be transmitted over LAN. Alarms are only reported against entities that are IS.*

If LAN type is 10Base2, check LAN wiring [DLP-020] and provisioning at other NEs in the LAN network. To correct provisioning errors, return to step 4.

14 Was the problem found and corrected?

If yes, STOP. This procedure is complete.
If no, go to step 15.

15 Replace NEP per DLP-101; then retrieve alarms [DLP-100].

16 Did CARLOS alarm clear?

If yes, STOP. This procedure is complete.
If no, contact Customer Service. All probable causes have been considered.

17 STOP. This procedure is complete.

Alarm/Condition – DUPADR

18 ***NOTE:*** *A duplicate address was encountered, which is a significant error. Once provisioning is eliminated as an alarm cause, options are limited. Perform some preliminary research to help Customer Service isolate the direct cause of the alarm, or contact Customer Service as soon as alarm is received.*

Do you want to conduct preliminary research?

If yes, go to step 19.
If no, go to step 22.

19 Retrieve all NSAPs in the level 1 routing table [DLP-550].

20 Compare the NSAPs in the level 1 routing table to ensure that there are no duplications. Record if found.

21 Retrieve alarms to verify that alarm is still activated [DLP-100].

22 Contact Customer Service.

23 STOP. This procedure is complete.

TAP-045
Clear LLSMLDCC (EOC) Alarm

Purpose

Provides procedures for clearing LLSMLDCC (EOC) alarm on SML facility.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

STEP	PROCEDURE
1	Retrieve alarms [DLP-100].
2	Are there any SML facility alarms? If yes, go to TAP-033. If no, go to step 3.
3	**NOTE:** *Conflict may exist in LLSMLDCC Side Role entries at the local NE and the far-end NE that terminates the alarmed EOC. A proper Side Role setting entry at both NEs must be made for each to establish EOC communication and retire EOC alarm. The Side Role value setting for one end of the link must be User Side, and the other end of the link must be set to Network Side. Other LLSMLDCC parameters should be the same at the two NEs. The primary state of the LLSMLDCC entity must be in-service (Service State = In Service) at both ends of the link.* **NOTE:** *If EOC communication is unavailable, remote logon to the remote NE may not be possible. You may have to go to the remote side and log on to retrieve and modify the Side Role entries.* Retrieve provisioned lower layer DCC data at the local NE [DLP-551] and check the service state and provisioning of the Side Role parameter.
4	Retrieve provisioned lower layer DCC provisioned data at the far-end NE that terminates the link [DLP-551] and check the service state and provisioning of the Side Role parameter.
5	Does Service State = In Service on both NEs and is the Side Role set to User Side on one NE and to Network Side on the other? If yes, go to step 9. If no, go to step 6.

6 Correct the provisioning and/or primary state for LLSMLDCC [DLP-551].

7 Retrieve alarms [DLP-100].

8 Did the EOC alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 9.

9 ***NOTE:*** *All probable causes have been considered.*

Look for other (obscure) alarm conditions which may indirectly be causing this alarm [TAP-001] or contact Customer Service.

10 STOP. This procedure is complete.

TAP-046
Clear TADRMap Alarm

Purpose

Provides a procedure for clearing a TADRMM alarm.

A TADRMM alarm indicates that the Target Identifier Address Resolution Map (TADRMap) contains a TID-to-NSAP pair that the network does not recognize.

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

STEP	PROCEDURE
1	Retrieve TADRMap alarms [DLP-100].
2	Analyze response and make a note of the component value (AID) associated with the alarm: where: Component = TADRMAP-1...TADRMAP-32
3	Delete TADRMAP pair identified by AID [DLP-508].
4	Retrieve TADRMap alarms [DLP-100].
5	Did alarm clear? If yes, STOP. This procedure is complete. If no, go to step 6.
6	Look for other (obscure) alarm conditions which may indirectly be causing this alarm [TAP-001] or contact Customer Service.
7	STOP. This procedure is complete.

TAP-047
Clear IP Tunnel Alarm

Purpose

Provides a procedure for clearing an IP Tunnel EOC (Embedded Operations Channel) alarm.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Check the setting of the IP Tunnel Link Establishment Mode: a. In the scope pane, expand System; then expand Network Features and select IP Tunnel. b. In the result pane, note the setting of the Link Establishment Mode for the remote NE.
2	Is the mode set correctly for the remote NE (i.e., SMX or SM9)? If yes, go to step 6. If no, go to step 3.
3	Change the Link Establishment Mode: a. In the result pane, right-click IPT that is generating the EOC alarm. b. From the context menu that is displayed, select **Provision Parameters** to open a work view. c. From the Link Establishment Mode drop-down list, select the correct mode for the remote NE. d. On the toolbar, select Submit; then close work view.
4	Retrieve alarms [DLP-100].
5	Did the alarm clear? If yes, STOP. This procedure is complete. If no, go to step 6.
6	Re-establish IP Tunnel. Refer to the 1603 SMX Provisioning Guide.
7	STOP. This procedure is complete.

TAP-048
Clear Power Distribution Unit (PDU) Alarm

Purpose

Provides procedures for clearing Power Distribution Unit (PDU) alarms.

STEP	PROCEDURE
1	Identify the alarm (see Figure 1). If it is the Fuse alarm, go to step 2. If it is the Critical, Major or Minor alarm, go to step 8.

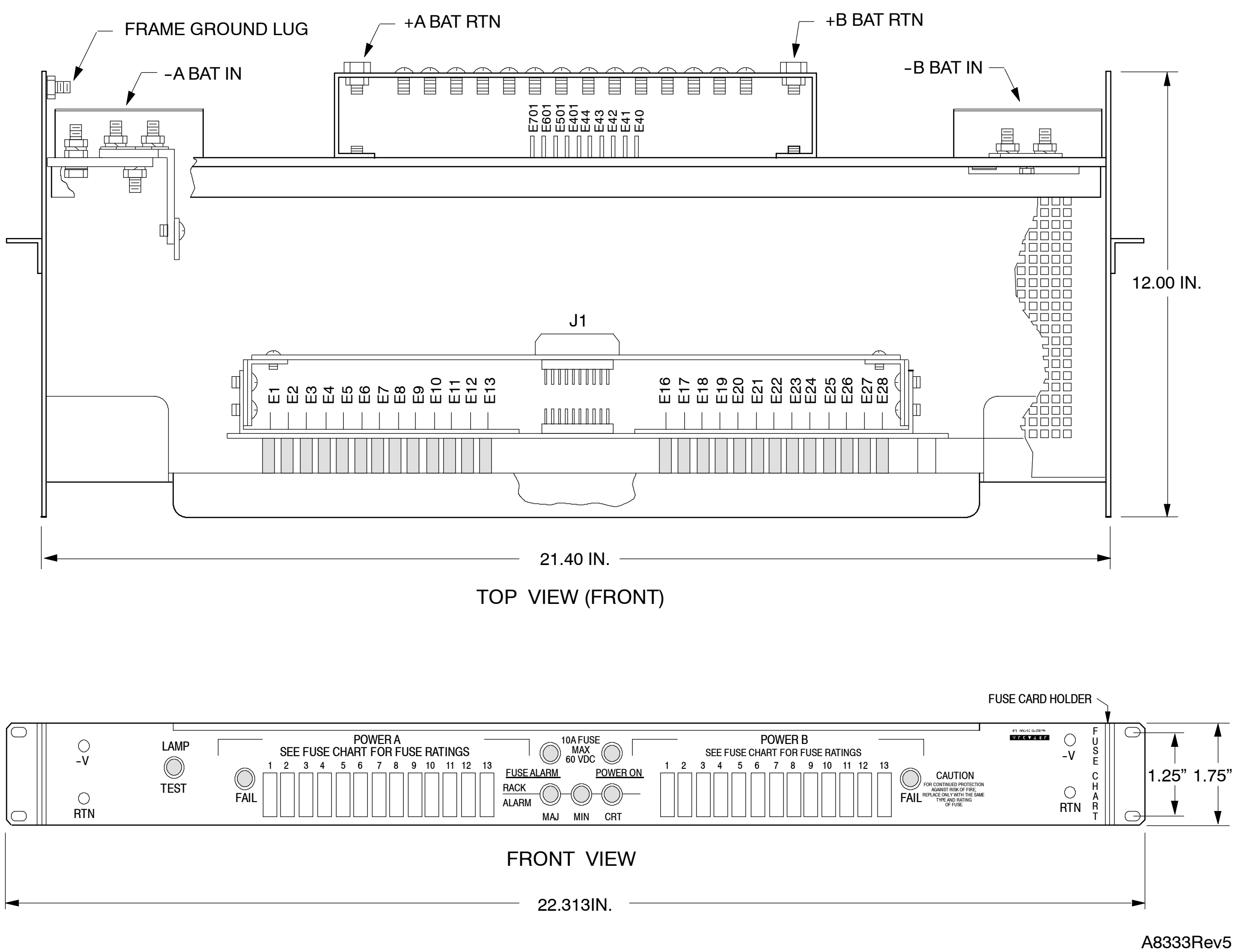


Figure 1. PDU113 Front and Top Views

FUSE Alarm

2 See Figure 1. Look for blown fuse on the fuse distribution panel.

3 Remove blown fuse and identify amperage or color.

4 Place good fuse in holder.

5 Did the new fuse blow?

If yes, go to step 6.
If no, STOP. This procedure is complete.

6 Check configuration chart for what the fuse supplies and resolve that unit's problem; check for shorts with a DVM or equivalent.

7 STOP. This procedure is complete.

CRITICAL/MAJOR/MINOR Alarms

8 Examine the modules being served by the fuse panel (see configuration chart attached to front of fuse panel, Figure 1).

9 Inspect the COA unit and NEP unit on each module for critical, major or minor alarms.

10 With a craft terminal connected to the COA, log on to the NE [DLP-117] and retrieve alarms [DLP-100].

11 From the response, identify unit and clear alarm; go to IXL-001.

12 STOP. This procedure is complete.

TAP-050
Clear DS1 Facility Alarm (DS3/DS1 Transmux)

Purpose

Provides procedures for clearing DS1 alarms for drop group equipped with LIF601.

General

This procedure assumes you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Retrieve alarms [DLP-100].
2	Are there any LIF, LDR, or DS3 alarms on the drop group with the alarmed DS1? If yes, go to TAP-001 and clear these alarms. If no, go to step 3.
3	Is far-end DS1 terminal a 1603 SMX, 1603 SM, or 1603 SE network element? If yes, go to step 5. If no, go to step 4.
4	Go to far-end terminal and resolve equipment alarms per vendor's documentation. If no problems are found, go to step 7.
5	Retrieve alarms at far-end NE [DLP-100].
6	Are there any equipment alarms? If yes, go to TAP-021 to clear alarm(s). If no, go to step 7.
7	Have DS1 alarms and conditions been retrieved? If yes, go to step 9. If no, go to step 8.

8 Retrieve DS1 alarms and conditions [DLP-100].

9 Identify the alarm condition and Access Identifier (refer to Table A); then go to the step indicated in Table B to clear alarm.

Table A. DS1 (T1)-to-VT1 Assignment (Sequential and Grouped AID Formats)

	DS2 1				DS2 2				DS2 3				DS2 4				DS2 5				DS2 6				DS2 7			
T1 SEQ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
VT1.5 SEQ	1	8	15	22	2	9	16	23	3	10	17	24	4	11	18	25	5	12	19	26	6	13	20	27	7	14	21	28
VT1.5 and T1 GRP	1-1	1-2	1-3	1-4	2-1	2-2	2-3	2-4	3-1	3-2	3-3	3-4	4-1	4-2	4-3	4-4	5-1	5-2	5-3	5-4	6-1	6-2	6-3	6-4	7-1	7-2	7-3	7-4

* *The AID format used is determined by the provisionable setting of the VT1.5/DS1 Numbering Mode parameter (System>General>Global).*

Table B. DS1 Facility (Transmux) Alarms/Conditions/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
AIS	Alarm Indication Signal (NEND RCV). An alarm condition has been detected from upstream.	10
DS2OOF	A DS2 out-of-frame has been detected at the receiver. A probable cause is misprovisioning of the DS3 frame format at either end of DS3 facility.	12
DS2RAI	DS2 Remote Alarm Indication. A failure at the far end resulted in the transmission of a continuous RAI signal in the reverse direction (i.e., toward the near-end NE) via the DS2 X-bits.	45
INHLPBK-( )	Inhibit loopback (DS2, ESFLINE, FEAC)	51
INHPMREPT	Performance monitoring reporting is inhibited	53
LOF	Loss of Frame (NEND RCV). An out-of-frame condition has persisted for more than 3 ms plus alarm delay time.	55
MTCE	Removed from service for maintenance	59
RAI	Remote Alarm Indication (NEND RCV). Failures such as LOS, LOF, and AIS at the far end result in the transmission of a continuous RAI signal in the reverse direction (i.e., toward the near-end NE). The RAI replaces the yellow alarm and is only applicable to SF and ESF formats.	61
T-CSSP	Controlled slip seconds – Path TCA* (FEND RCV)	64

Table B. DS1 Facility (Transmux) Alarms/Conditions/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
T-CVP	Coding violations – Path TCA* (NEND RCV)	64
	Coding violations – Path TCA* (FEND RCV)	64
T-ESL	Error seconds – Line TCA* (FEND RCV)	64
T-ESP	Error seconds – Path TCA* (NEND RCV)	64
	Error seconds – Path TCA* (FEND RCV)	64
T-SASP	SEF/AIS seconds – Path TCA* (NEND RCV)	64
T-SEFS	Severely errored framing seconds TCA* (FEND RCV)	64
T-SESP	Severely errored seconds – Path TCA* (NEND RCV)	64
	Severely errored seconds – Path TCA* (FEND RCV)	64
T-UASP	Unavailable seconds – Path TCA* (NEND RCV)	64
	Unavailable seconds – Path TCA* (FEND RCV)	64
Condition	**Description**	**Action**
ACTLPBK	Loopback is active (Loopback type, location, request types are displayed as comment)	No Action
AINS	Automatic In-Service	No Action
Event	**Description**	**Action**
ACTLPBK	Loopback is activated	No Action
AINS	Automatic In-Service	No Action
IS-AUTO	Automatic OOS-MA to IS	No Action
* *TCA = Threshold Crossing Alert*		

Alarm/Condition – AIS

10 ***NOTE:*** *AIS is received on an incoming (input, mux direction) DS1.*

Troubleshoot far-end equipment and DS3 facility.

11 STOP. This procedure is complete.

Alarm/Condition – DS2OOF

12 **CAUTION: Possibility of service interruption exists when replacing an LIF or LDR. To avoid service interruption, adhere to the replacement procedure in DLP-101.**

13 Retrieve DS3 port parameters [DLP-502].

14 Is DS3 Format parameter provisioned correctly per office records?

If yes, go to step 17.
If no, go to step 15.

15 Change provisioning of DS3 Format parameter to agree with office records [DLP-502].

16 Check far-end equipment for frame format type. Correct if necessary.

17 Retrieve alarms [DLP-100].

18 Did alarm clear (may take several minutes)?

If yes, STOP. This procedure is complete.
If no, go to step 19.

19 At the NE with the alarm, is the LIF/LDR configuration redundant for the alarmed DS1?

If yes, go to step 20.
If no (non-redundant), go to step 30.

20 Perform duplex switching of the LIFs [DLP-505]; then retrieve alarms [DLP-100].

21 Did alarm clear (may take several minutes)?

If yes, go to step 22.
If no, go to step 24.

22 Replace standby LIF per DLP-101.

23 STOP. This procedure is complete.

24 Perform duplex switching of the LDRs [DLP-505]; then retrieve alarms [DLP-100].

25 Did alarm clear (may take several minutes)?

If yes, go to step 26.
If no, go to step 28.

26 Replace standby LDR per DLP-101.

27 STOP. This procedure is complete.

28 ***NOTE:*** *Problem must be at far-end DS1 terminal.*

Check for alarms at far-end NE [DLP-100]. If no alarms are detected and problem continues, test DS3 coax facility per local procedure or contact Customer Service.

29 STOP. This procedure is complete.

30 **CAUTION: Possibility of service interruption. Service-affecting diagnostics will be performed on the LIF and LDR units. If DS1 is carrying traffic with no service-affecting problems, perform diagnostics when traffic volume is low.**

31 Place LIF to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

32 Run all diagnostic phases on LIF [DLP-500]. Perform one iteration.

33 Did diagnostics pass?

If yes, go to step 36.
If no, go to step 34.

34 Replace LIF per DLP-101.

35 STOP. This procedure is complete.

36 Place LIF back in-service [DLP-501].

37 Place LDR to be tested in maintenance state (OOS-MT-MAN) [DLP-501].

38 Run all diagnostic phases on LDR [DLP-500]. Perform one iteration.

39 Did diagnostics pass?

If yes, go to step 42.
If no, go to step 40.

40 Replace LDR per DLP-101.

41 STOP. This procedure is complete.

42 Place LDR back in-service [DLP-501].

43 ***NOTE:*** *Problem must be at far-end terminal.*

Check for alarms at far-end NE [DLP-100]. If no alarms are detected and problem continues, test coax facility per local procedure or contact Customer Service.

44 STOP. This procedure is complete.

Alarm/Condition – DS2RAI

45 ***NOTE:*** *The DS2 RAI is detected upon demultiplexing the received DS3 signal.*

Check far-end NE for service-affecting equipment or facility alarms [DLP-100]. Clear any alarms that are present.

46 Were any alarms found (and cleared) at far-end NE?

If yes, go to step 47.
If no, go to step 49.

47 Retrieve alarms at near-end NE [DLP-100].

48 Did DS2RAI alarm clear (may take several minutes to clear)?

If yes, STOP. This procedure is complete.
If no, go to step 49.

49 Go to step 19 and test LIF and LDR at near-end NE.

50 STOP. This procedure is complete.

Alarm/Condition – INHLPBK

51 To clear alarm, allow remote activation of loopback on DS1 [DLP-548].

52 STOP. This procedure is complete.

Alarm/Condition – INHPMREPT

53 To clear alarm, allow PM reporting on DS1 [DLP-510].

54 STOP. This procedure is complete.

Alarm/Condition – LOF

55 Retrieve DS1 port parameters at both ends of the DS1 circuit [DLP-502].

56 Is DS1 Format parameter provisioned the same at both ends?

If yes, go to step 19 and test LIF and LDR at near end.
If no, go to step 57.

57 Change provisioning of DS1 Format parameter to agree with office records [DLP-502].

58 STOP. This procedure is complete.

Alarm/Condition – MTCE

59 To clear alarm, place DS1 back in-service [DLP-502].

60 STOP. This procedure is complete.

Alarm/Condition – RAI

61 RAI is received on incoming (input, mux direction) DS1. Check for and clear equipment or DS3 facility alarms at far end [TAP-001].

62 Did alarm clear (may take several minutes to clear)?

If yes, then go to step 63.
If no, go to step 19 and test LIF and LDR at near end.

63 STOP. This procedure is complete.

Alarm/Condition – T-xxx

64 Retrieve T3 conditions [DLP-100].

65 Are there any DS3 alarms or conditions?

If yes, go to TAP-043.
If no, go to step 66.

66 A threshold crossover alert has been generated because one of the performance parameters exceeds the value specified for it (refer to Table C).

67 Retrieve current conditions for DS1 facility [DLP-100].

68 Are there any other DS1 facility alarms (besides T-xxx)?

If yes, go to step 69.
If no, go to step 71.

69 Correct other facility alarms before resolving T-xxx conditions. Refer to Table B.

70 STOP. This procedure is complete.

71 Is the condition severe enough to warrant unit replacement?

If yes, go to step 73.
If no, record the alarm as an event.

72 STOP. This procedure is complete.

Table C. DS1 (DS3/DS1 Transmux) PM Thresholds

MONITOR TYPE	FACTORY DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
BERL-HT	4		3...6	Bit error ratio line – High threshold (SFBER)
BPV	13340	133400	1...4,294,967,295	Bipolar violations
CSSP	1	4	1...65535	Controlled slips
CVL	13340	133400	1...4,294,967,295	Coding violation count – Line
CVP (FMT=SF)	72	691	1...4,294,967,295	Coding violation count – Path
CVP (FMT=ESF)	13296	132960	1...4,294,967,295	Coding violation count – Path
ESL	65	648	1...65535	Line Errored Seconds
ESP	65	648	1...65535	Path Errored Seconds
SASP	2	17	1...65535	Path AIS seconds
SEFS	2	17	1...65535	Severely errored framing seconds (OOFS/COFAS)
SESL	10	100	1...65535	Line Severely Errored Seconds
SESP	10	100	1...65535	Path Severely Errored Seconds
UASP	10	10	1...65535	Unavailable seconds – Path

73 From the work view opened in step 67, determine Direction of T-xxx condition. (See Figure 1 for definition of Location (NEND/FEND) parameters.)

74 Is location specified near end (NEND) or far end (FEND)?

If NEND, go to step 75.
If FEND, go to step 76.

75 ***NOTE:*** *A near-end location indicates errors are detected on received embedded DS1.*

Troubleshoot far-end M13 Line Terminating Equipment (LTE), far end DS1 facility and equipment; then go to step 77.

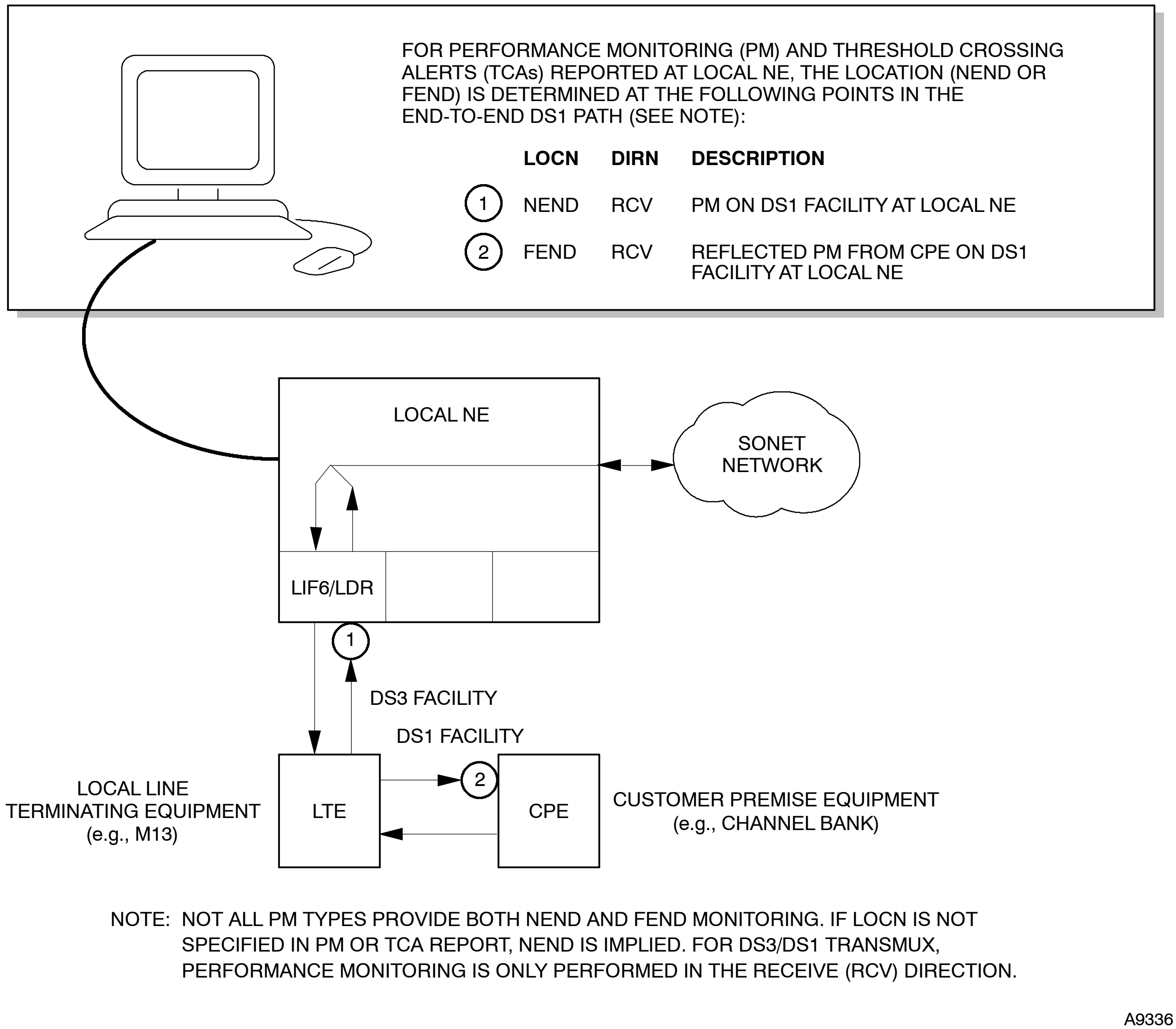


Figure 1. PM Monitoring Points in DS1 Circuit (DS3/DS1 Transmux)

76 **NOTE:** *A far-end location indicates that far-end DS1 equipment (channel bank, CPE, etc.) is detecting errors on the incoming DS1 facility and reporting them over the PRM (Performance Report Message) channel back to local NE. Suspect far end LTE (M13), DS1 facility or local NE.*

Troubleshoot facility and LTE per local practice.

NOTE: *If trouble is not found, problem may be at local NE.*

77 Was problem found and corrected?

If yes, STOP. This procedure is complete.
If no, go to step 78 to troubleshoot local NE.

78 Retrieve DS1 port parameters [DLP-502].

79 Does provisioned value of DS1 Format parameter match office records?

If yes, go to step 82.
If no, go to step 80.

80 Change provisioning of DS1 Format parameter to agree with office records [DLP-502].

81 STOP. This procedure is complete.

82 At the NE with the alarm, is the LIF/LDR configuration redundant for the alarmed DS1?

If yes, go to step 83.
If no (non-redundant), go to step 30 and diagnose LIF and LDR.

83 Perform duplex switching of the redundant LIFs [DLP-505].

84 Retrieve PM registers [DLP-517].

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves register values.*

85 Did PM error stop?

If yes, go to step 86.
If no, go to step 88.

86 Replace standby LIF per DLP-101.

87 STOP. This procedure is complete.

88 Perform duplex switching of the redundant LDRs [DLP-505].

89 Retrieve PM registers [DLP-517].

90 Did PM error stop?

If yes, go to step 91.
If no, go to step 93.

91 Replace standby LDR per DLP-101.

92 STOP. This procedure is complete.

93 ***NOTE:*** *Problem must be in facility or at far-end equipment.*

Troubleshoot per local practice.

94 If problem persists, contact Customer Service.

95 STOP. This procedure is complete.

TAP-051
Clear ATM Port Alarm

Purpose

Provides procedures for clearing ATM Port alarms.

General

This procedure assumes that you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Have alarms and conditions been retrieved? If yes, go to step 3. If no, go to step 2.
2	Retrieve ATM Port alarms and conditions [DLP-100]. ***NOTE:*** *Figure 1 identifies the location in the network where an ATM Port alarm is reported.*
3	Locate the alarm you want to clear in Table A; then go to step indicated to clear it.

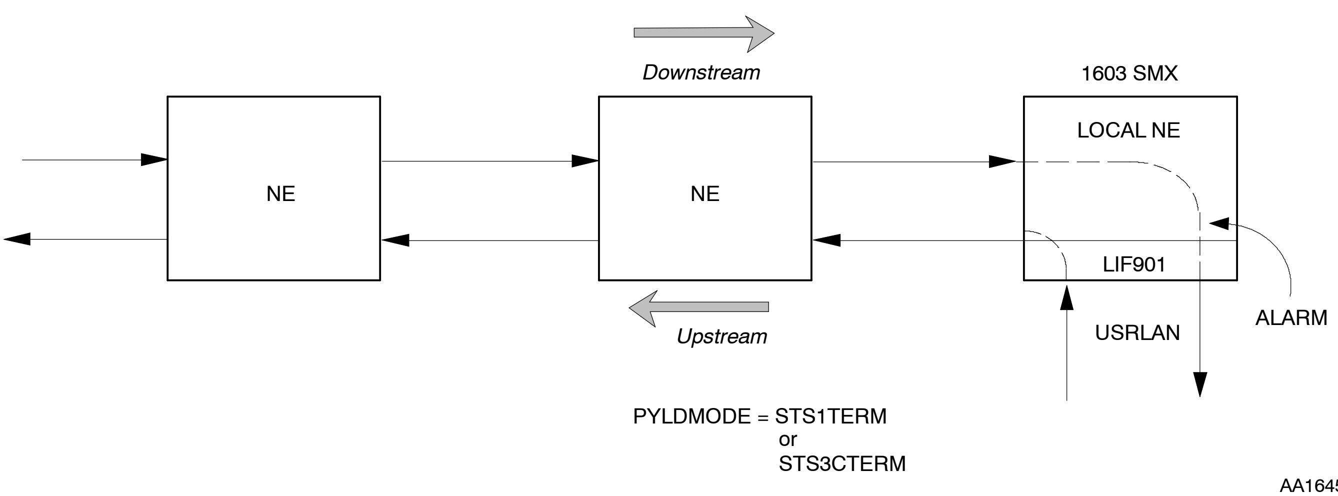


Figure 1. ATMPORT Alarms on NE Equipped with LIF901

Table A. Alarms/Conditions

ALARM/CONDITION	REASON FOR ALARM	STEP
INCOMPATGFC	Incompatible Generic Flow Control (GFC) protocol error. One possible cause is that the far-end NE sending the ATM cells is using GFC, which 1603 SMX does not support. Another possible cause is that the ATM Port has been incorrectly provisioned as a UNI.	4
INHPMREPTNDC	Reporting of scheduled Network Data Collection (NDC) PM reports has been inhibited.	6
INHPMREPTQOS	Reporting of scheduled Quality of Service (QOS) PM reports has been inhibited	8
LCD	Loss of Cell Delineation. ATM cell boundaries can no longer be identified. The most likely cause for this type of alarm is an equipment or facility failure. This alarm could also be caused by missing STS1 or STS3c connections in the network.	10
T-CDHDRVP	The threshold for cells discarded due to ATM layer header errors in VPI field has been exceeded.	23
T-CDHEC	The threshold for cells discarded due to Header Error Check (HEC) violations has been exceeded. There are a number of SONET failures that could cause these alarms.	25

Alarm/Condition – INCOMPATGFC

4 Check provisioning of ATM cell source at far-end NE.

5 STOP. This procedure is complete.

Alarm/Condition – INHPMREPTNDC

6 To clear alarm, allow scheduled NDC reports [DLP-510].

7 STOP. This procedure is complete.

Alarm/Condition – INHPMREPTQOS

8 To clear alarm, allow scheduled QOS reports [DLP-510].

9 STOP. This procedure is complete.

Alarm/Condition – LCD

10 At the local NE, check for equipment or SYNC alarms [DLP-100].

11 Are there any equipment or SYNC alarms?

If equipment alarms, go to TAP-021.
If SYNC alarms, go to TAP-027.
If neither of these alarms, go to step 12.

12 Retrieve conditions on the STS1 or STS3c path associated with ATM Port [DLP-100].

13 Check for AISP, LOP, PLM, UNEQ, BERP-LT, BERP-HT, or any T-xxx conditions. Do any of these conditions exist on the STS path?

If yes, go to TAP-034 to clear alarms.
If no, go to step 14.

14 At the upstream NE where the ATM cells are mapped onto the STS1 or STS3c path, check for equipment or SYNC alarms [DLP-100].

15 Are there any equipment or SYNC alarms?

If equipment alarms, go to TAP-021 to clear alarms.
If SYNC alarms, go to TAP-027 to clear alarms.
If neither of these alarms, go to step 16.

16 At the NE upstream from the local NE, verify cross-connection for STS1 or STS3c path [DLP-504].

17 Is the cross-connection for the path in place?

If yes, go to step 19.
If no, go to step 18.

18 Re-establish path cross-connect [DLP-504].

19 Verify path cross-connections back to the point where the ATM cells are mapped into the STS1 or STS3c path.

20 Were any bad STS path cross-connections found?

If yes, reestablish path cross-connects [DLP-504].
If no, go to step 21.

21 If problem persists, contact Customer Service.

22 STOP. This procedure is complete.

Alarm/Condition – T-CDHDRVP

23 Check provisioning of ATM cell source at far-end NE.

24 STOP. This procedure is complete.

Alarm/Condition – T-CDHEC

25 Check for equipment alarms or a SYNC alarm [DLP-100].

26 Are there any equipment or SYNC alarms?

If equipment, go to TAP-021 to clear alarms.
If SYNC, go to TAP-027 to clear alarms.
If neither of these alarms, then go to step 27.

27 Retrieve conditions on the STS1 or STS3c path associated with the ATM Port [DLP-100].

28 Check for T-xxx conditions on the STS path. Do any of these conditions exist?

If yes, go to TAP-034 to clear alarms.
If no, go to step 29.

29 If problem persists, contact Customer Service.

30 STOP. This procedure is complete.

TAP-052
Clear ATM Processor Alarm

Purpose

Provides procedures for clearing ATM Processor alarms.

General

This procedure assumes that you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Have alarms and conditions been retrieved? If yes, go to step 3. If no, go to step 2.
2	Retrieve ATM Processor alarms and conditions [DLP-100].
3	Find alarm in Table A; then go to the step indicated to clear alarm.

Table A. Alarms/Conditions

ALARM/CONDITION	REASON FOR ALARM	STEP
INHPMREPTNDC	Reporting of scheduled Network Data Collection PM reports has been inhibited.	4
INHPMREPTNTM	Reporting of scheduled Network Traffic Management PM reports has been inhibited.	6
INHPMREPTQOS	Reporting of scheduled Quality of Service PM reports has been inhibited.	8
T-CDCRC10	The number of OAM cells discarded due to errors detected by the CRC-10 Error Detection Code has exceeded the threshold.	10
T-CDINVLD	The number of OAM cells discarded due to invalid values (i.e., invalid OAM cell type, unsupported OAM function type, and invalid function specific fields) has exceeded the threshold.	19
T-CDCONG0+1	The number of high and low priority cells being discarded due to congestion has exceeded the provisioned threshold. Cells are being discarded because the amount of traffic received from the AAL5 layer towards the CCM exceeds the capacity of the STS signal towards the cross-connect.	21
T-CDCONGPROC	The number of OAM cells being discarded due to congestion in OAM processing has exceeded the provisioned threshold.	23

Alarm/Condition – INHPMREPTNDC

4 To clear alarm, allow reporting of scheduled ATM Processor NDC PM reports [DLP-510].

5 STOP. This procedure is complete.

Alarm/Condition – INHPMREPTNTM

6 To clear alarm, allow reporting of scheduled ATM Processor NTM PM reports [DLP-510].

7 STOP. This procedure is complete.

Alarm/Condition – INHPMREPTQOS

8 To clear alarm, allow reporting of scheduled ATM Processor QOS PM reports [DLP-510].

9 STOP. This procedure is complete.

Alarm/Condition – T-CDCRC10

10 Retrieve ATM Port conditions [DLP-100].

11 Are there any ATM Port T-CDHEC conditions?

If yes, go to TAP-051.
If no, go to step 12.

12 Check for equipment or SYNC alarms [DLP-100].

13 Are there any equipment alarms?

If yes, go to TAP-021.
If no, go to step 14.

14 Are there any SYNC alarms?

If yes, go to TAP-027.
If no, go to step 15.

15 Retrieve conditions on the STS1 and STS3c paths [DLP-100].

16 Check for BERP-LT, BERP-HT, or T-xxx conditions. Do any of these conditions exist?

If yes, go to TAP-034.
If no, go to step 17.

17 If problem persists, contact Customer Service.

18 STOP. This procedure is complete.

Alarm/Condition – T-CDINVLD

19 ***NOTE:*** *The most likely cause is an improper setup at the NE originating the ATM cells.*

Check the setup at the NE originating the ATM cells.

20 STOP. This procedure is complete.

Alarm/Condition – T-CDCONG0+1

21 The following are some actions that traffic engineering can take to clear the alarm:

a. Provision additional bandwidth by using STS3TERM payload mode.

b. Reduce the number of USRLAN facilities.

c. Modify the traffic profile associated with VP's carrying the ATM traffic [DLP-530].

22 STOP. This procedure is complete.

Alarm/Condition – T-CDCONGPROC

23 Are there any T-CDCONG0+1 conditions?

If yes, go to step 21.
If no, go to step 24.

24 If problem persists, contact Customer Service.

25 STOP. This procedure is complete.

TAP-053
Clear VPL Alarm

Purpose

Provides procedures for clearing VPL alarms.

General

This procedure assumes that you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Have alarms and conditions been retrieved? If yes, go to step 3. If no, go to step 2.
2	Retrieve VPL alarms and conditions [DLP-100].
3	Find alarm in Table A and go to step indicated to clear alarm.

Table A. Alarms/Conditions/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
AIS (rcv)	VP AIS cells are being received because a failure occurred somewhere upstream.	4
INHCONTCE	Remote activation of VP connection continuity check has been inhibited.	18
INHCONTSE	Remote activation (rcv & trmt) of VP segment endpoint continuity check has been inhibited.	20
INHPMCE	Remote activation of VP connection performance monitoring has been inhibited.	22
INHPMREPTCQOS	Reporting of scheduled VP connection QOS performance monitoring reports has been inhibited.	24
INHPMREPTSQOS	Reporting of scheduled VP segment QOS performance monitoring reports has been inhibited.	26

Table A. Alarms/Conditions/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
INHPMSE	Remote activation (rcv & trmt) of VP segment performance monitoring has been inhibited.	28
LOSSCONTCE	Loss of VP Connection Continuity. The connection between the source NE and the sink NE may have been lost.	30
LOSSCONTSE	Loss of VP Segment Continuity. The connection between segment endpoints may have been lost.	46
RFI	Remote Failure Indication. An LIF901 that is a VPL connection endpoint has detected VP RDI.	62
T-IMP0+1	Threshold violation for 0+1 impaired cell blocks	73
T-SECB	Threshold violation for severely errored cell blocks	73
T-TLOS0	Threshold violation for total lost 0 user information cells	73
T-TLOS0+1	Threshold violation for total lost 0+1 user information cells	73
Condition	**Description**	**Action**
AISLOC	VPAIS defect location displayed as a comment	*
ACTBKWDRPTCE (NE)	VP connection backward reporting PM cells being transmitted	No action
ACTBKWDRPTCE (FE)	VP connection backward reporting PM cells being received	No action
ACTBKWDRPTSE (NE)	VP segment backward reporting PM cells being transmitted	No action
ACTBKWDRPTSE (FE)	VP segment backward reporting PM cells being received	No action
ACTCONTCE (NE)	VP connection continuity cells being transmitted	No action
ACTCONTCE (FE)	VP connection continuity cells being received	No action
ACTCONTSE (NE)	VP segment continuity cells being transmitted	No action
ACTCONTSE (FE)	VP segment continuity cells being received	No action
ACTFWDMONCE (NE)	VP connection forward monitoring PM cells being transmitted	No action
ACTFWDMONCE (FE)	VP connection forward monitoring PM cells being received	No action

Table A. Alarms/Conditions/Events (cont)

Condition	**Description**	**Action**
ACTFWDMONSE (NE)	VP segment forward monitoring PM cells being transmitted	No action
ACTFWDMONSE (FE)	VP segment formward monitoring PM cells being received	No action
RDILOC	VPL RDI location ID	*
Event	**Description**	**Action**
ACTBKWDRPTCE (NE)	VP connection backward reporting PM cells being transmitted	No action
ACTBKWDRPTCE (FE)	VP connection backward reporting PM cells being received	No action
ACTBKWDRPTSE (NE)	VP segment backward reporting PM cells being transmitted	No action
ACTBKWDRPTSE (FE)	VP segment backward reporting PM cells being received	No action
ACTCONTCE (NE)	VP connection continuity cells being transmitted	No action
ACTCONTCE (FE)	VP connection continuity cells being received	No action
ACTCONTSE (NE)	VP segment continuity cells being transmitted	No action
ACTCONTSE (FE)	VP segment continuity cells being received	No action
ACTFWDMONCE (NE)	VP connection forward monitoring PM cells being transmitted	No action
ACTFWDMONCE (FE)	VP connection forward monitoring PM cells being received	No action
ACTFWDMONSE (NE)	VP segment forward monitoring PM cells being transmitted	No action
ACTFWDMONSE (FE)	VP segment forward monitoring PM cells being received	No action
* *Troubleshoot VPL alarm/condition on same VPL facility.*		

Alarm/Condition – AIS

NOTE: *A failure occurring somewhere upstream has been detected on a drop group VPL. Since the failure could have occurred at any one of a number of NEs in the network, troubleshooting this alarm involves investigating each NE on the upstream path.*

NOTE: *Failures that trigger VP AIS generation are failures detected at an ATMPORT or a VPL in the downstream direction; however, the NE reporting the AIS condition may not be experiencing any failures. Figure 1 shows a possible defect location that could cause a VPL AIS to occur.*

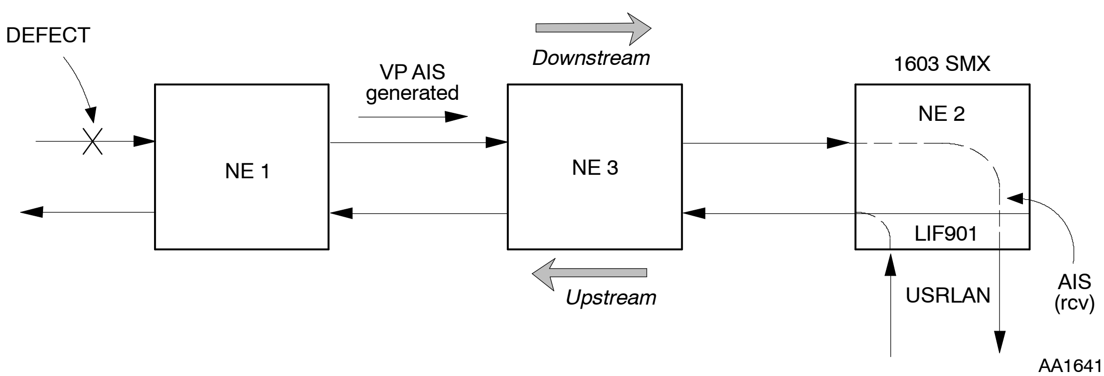


Figure 1. VP AIS Defect Flow (LIF901)

4 Retrieve VPL alarms and conditions [DLP-100].

5 Is an AISLOC condition reported for this VPL?

If yes, go to step 8.
If no, go to step 6.

6 Retrieve alarms at the local NE [DLP-100].

7 Is the local NE reporting an LCD alarm on any ATM Port associated with this VPL?

If yes, go to TAP-051.
If no, go to step 12.

8 Select AISLOC and click Details to retrieve information that identifies the NE sourcing the AIS alarm.

9 Retrieve alarms at the identified NE [DLP-100].

10 Is identified NE reporting an LCD alarm on any ATM Port associated with this VPL?

If yes, go to TAP-051.
If no, go to step 11.

11 Is the VPL reporting an LOSSCONTSE alarm?

If yes, go to step 46.
If no, go to step 12.

12 Retrieve alarms at the next upstream NE [DLP-100].

13 Is upstream NE reporting an LCD alarm on any ATM Port associated with this VPL (in the downstream direction)?

If yes, go to TAP-051.
If no, go to step 14.

14 Is upstream NE reporting a VPL LOSSCONTSE alarm (in the downstream direction)?

If yes, go to step 48.
If no, go to step 15.

15 Is this the last upstream NE?

If yes, go to step 16.
If no, return to step 12.

16 Contact Customer Service.

17 STOP. This procedure is complete.

Alarm/Condition – INHCONTCE

18 To clear alarm, allow remote activation of VPL connection continuity check [DLP-555].

19 STOP. This procedure is complete.

Alarm/Condition – INHCONTSE

20 To clear alarm, allow remote activation of VPL segment continuity check [DLP-555].

21 STOP. This procedure is complete.

Alarm/Condition – INHPMCE

22 To clear alarm, allow remote activation of VPL connection performance monitoring [DLP-556].

23 STOP. This procedure is complete.

Alarm/Condition – INHPMREPTCQOS

24 To clear alarm, allow scheduled connection QOS performance monitoring reports [DLP-510].

25 STOP. This procedure is complete.

Alarm/Condition – INHPMREPTSQOS

26 To clear alarm, allow scheduled segment QOS performance monitoring reports [DLP-510].

27 STOP. This procedure is complete.

Alarm/Condition – INHPMSE

28 To clear alarm, allow remote activation of segment performance monitoring [DLP-556].

29 STOP. This procedure is complete.

Alarm/Condition – LOSSCONTCE

NOTE: *The NE reporting this alarm has been designated as a sink for an ATM connection continuity check. See Figure 2. The alarm indicates that the connection between the source NE and the sink NE may have been lost.*

NOTE: *Both the source NE and the sink NE must be connection endpoints.*

NOTE: *There are several reasons why the connection may have been lost: a failure may have occurred in the network; a problem may exist with the cross-connection provisioning; or the continuity check may not have been set up properly.*

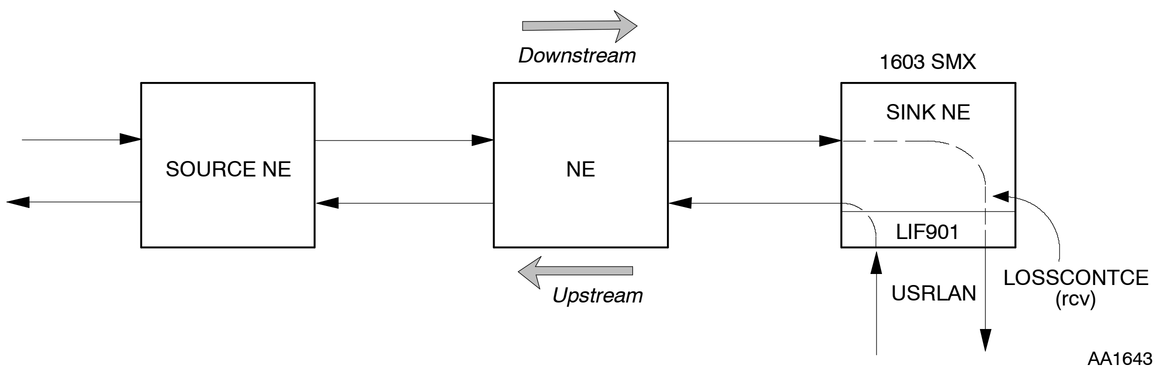


Figure 2. ATM Connection Continuity Check

30 Retrieve alarms at the local (sink) NE [DLP-100].

31 Is there an LCD on the ATM Port associated with alarmed VPL at the local NE?

If yes, go to TAP-051.
If no, go to step 32.

32 Retrieve VPL conditions at the local (sink) NE [DLP-100].

33 Is there an AIS condition in the downstream direction on this VPL?

If yes, go to step 34.
If no, go to step 43.

34 Is an AISLOC condition being reported for this VPL?

If yes, go to step 35.
If no, go to step 38.

35 Select AISLOC and click Details to retrieve information that identifies the NE sourcing the AIS alarm.

36 Retrieve alarms at the NE identified in step 35 [DLP-100].

37 Is the identified NE reporting an LCD alarm on any ATM Port associated with this VPL (in the downstream direction)?

If yes, go to TAP-051.
If no, go to step 38.

38 Retrieve alarms at the NE upstream from the local NE [DLP-100].

39 Is the upstream NE reporting an LCD on any ATM Port associated with this VPL (in the downstream direction)?

If yes, go to TAP-051.
If no, go to step 40.

40 Is this NE the connection endpoint NE?

If yes, go to step 41.
If no, return to step 38 and retrieve alarms for the next upstream NE.

41 Contact Customer Service.

42 STOP. This procedure is complete.

43 Retrieve VPL conditions at the continuity source NE [DLP-100].

44 Is ACTCONTCE being reported for this VPL?

If yes, verify continuity setup.
If no, reactivate continuity setup.

45 STOP. This procedure is complete.

Alarm/Condition – LOSSCONTSE

NOTE: *The NE reporting this alarm has been designated as a sink for an ATM segment continuity check. The alarm indicates that the connection between the source NE and the sink NE may have been lost. Both the source NE and the sink NE must be segment endpoints.*

NOTE: *There are several reasons why the connection may have been lost: a failure may have occurred in the network; a problem may exist with the cross-connection provisioning; or the continuity check may not have been set up properly.*

NOTE: *Figure 3 shows how a LOSSCONTSE alarm might occur.*

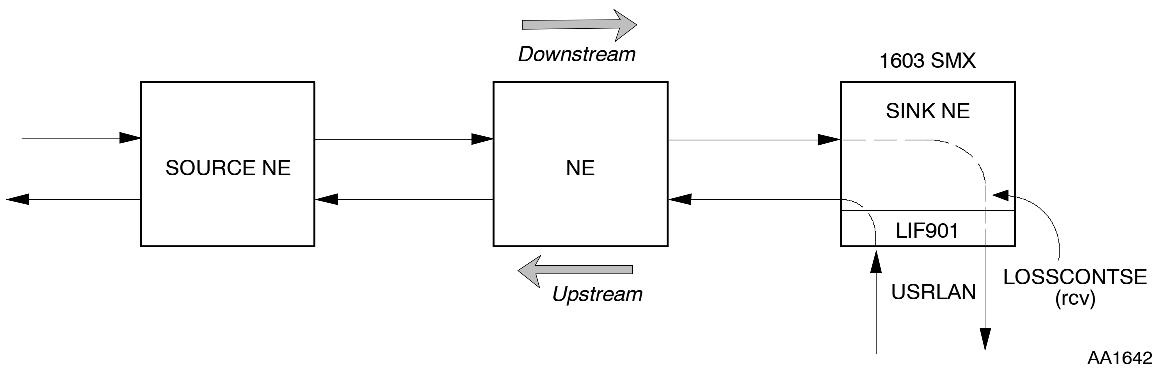


Figure 3. ATM Segment Continuity Check

46 Retrieve alarms at the local (sink) NE [DLP-100].

47 Is there an LCD on any ATM Port associated with alarmed VPL at the local NE?

If yes, go to TAP-051.
If no, go to step 48.

48 Retrieve VPL conditions at the local (sink) NE [DLP-100].

49 Is there an AIS condition in the downstream direction on this VPL?

If yes, go to step 50.
If no, go to step 59.

50 Is an AISLOC condition being reported for this VPL?

If yes, go to step 51.
If no, go to step 54.

51 Select AISLOC and click Details to retrieve information that identifies the NE sourcing the AIS alarm.

52 Retrieve alarms at the NE identified in step 51 [DLP-100].

53 Is the identified NE reporting an LCD alarm on any ATM Port associated with this VPL (in the downstream direction)?

If yes, go to TAP-051.
If no, go to step 54.

54 Retrieve alarms at the NE upstream from the local NE [DLP-100].

55 Is the upstream NE reporting an LCD on any ATM Port associated with this VPL (in the downstream direction)?

If yes, go to TAP-051.
If no, go to step 56.

56 Is this NE the segment endpoint NE?

If yes, go to step 57.
If no, return to step 54 and retrieve alarms for the next upstream NE.

57 Contact Customer Service.

58 STOP. This procedure is complete.

59 Retrieve VPL conditions at the continuity source NE [DLP-100].

60 Is ACTCONTSE being reported for this VPL?

If yes, verify continuity setup.
If no, reactivate continuity setup.

61 STOP. This procedure is complete.

Alarm/Condition – RFI

NOTE: *An RFI alarm is generated when an LIF901 that is a VPL connection endpoint detects VP RDI. The VP RDI is generated by the far end NE at the other end of the VPL connection when it detects VP AIS.*

62 Begin troubleshooting at the first NE that is upstream from the NE reporting the RFI alarm. (See Figure 4.)

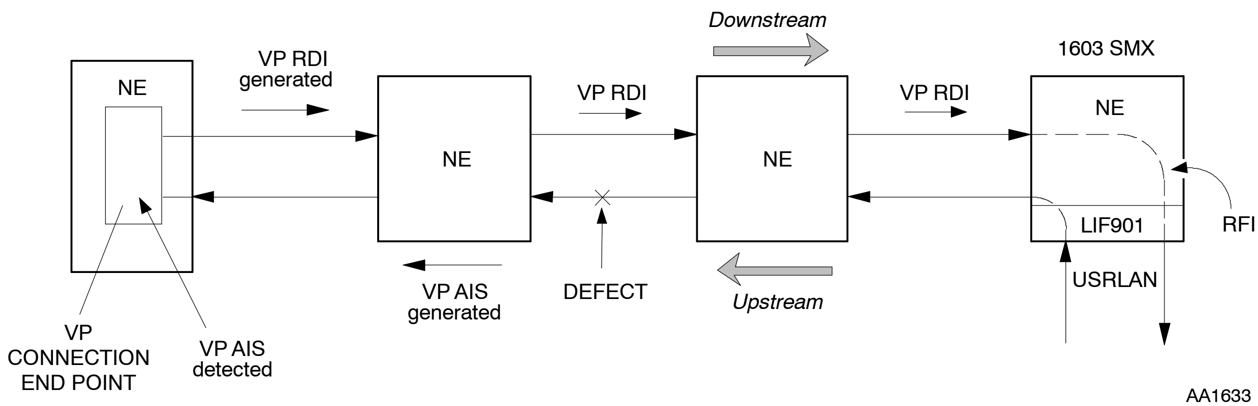


Figure 4. VPL RFI Alarm

63 Retrieve alarms at the first upstream NE [DLP-100].

64 Is the upstream NE reporting an LCD alarm in the upstream direction on any ATM Port associated with this VPL?

If yes, go to TAP-051.
If no, go to step 65.

65 Is the upstream NE reporting a VPL LOSSCONTSE alarm in the upstream direction?

If yes, go to step 46.
If no, go to step 66.

66 Retrieve alarms at the next upstream NE [DLP-100].

67 Is this NE reporting an LCD alarm in the upstream direction on any ATM Port associated with this VPL?

If yes, go to TAP-051.
If no, go to step 68.

68 Is this NE reporting a VPL LOSSCONTSE alarm in the upstream direction?

If yes, go to step 46.
If no, go to step 69.

69 Have alarms been retrieved at the VPL connection endpoint NE?

If yes, go to step 70.
If no, return to step 66.

70 Is the VPL connection endpoint NE reporting a VPL LOSSCONTCE alarm in the upstream direction?

If yes, go to step 32.
If no, go to step 71.

71 Contact Customer Service.

72 STOP. This procedure is complete.

Alarm/Condition – T-IMP0+1, T-SECB, T-TLOS0, or T-TLOS0+1

NOTE: *These performance parameters, which are accumulated at an LIF901, are collected to determine Quality-of-Service (QOS). Data is collected over blocks of ATM data cells between segment and collection endpoints. An alarm is generated when a specified threshold value is exceeded.*

73 Retrieve alarms [DLP-100].

74 On Alarm Surveillance work view, select (highlight) threshold alarm and select Details button to display Alarm Details screen.

75 On the Alarm Details screen, note location and direction of T-xxx alarm.

76 Find location and direction of alarm in Table B, and take appropriate action to clear the alarm. Figure 5 shows where the T-xxx alarm could occur and also helps determine the upstream and downstream directions.

Table B. Location and Direction of T–xxx Alarms

	LOCATION	DIRECTION	DESCRIPTION	ACTION TO TAKE
1*	NEND	RCV	Errors detected on VPL data received at local NE	Perform steps 77–88 to analyze failure in downstream direction. (See Figure 5.)
2*	FEND	RCV	Errors detected on VPL data received at remote NE and reported back to local NE	Perform steps 77–88 to analyze failure in upstream direction. (See Figure 5.)
* *This number refers to the location where errors are detected as shown on Figure 5.*				

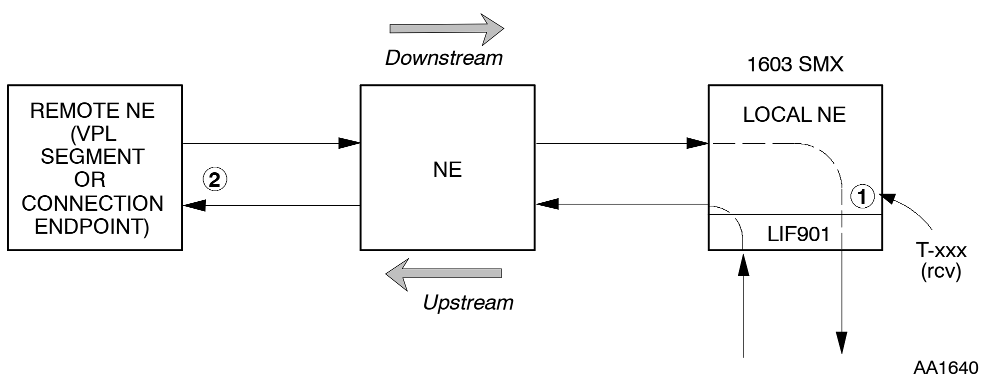


Figure 5. Receive NEND and FEND T-xxx on LIF901

77 Retrieve alarms at the local NE and check for equipment or SYNC alarms [DLP-100].

78 Are there any equipment alarms?

If yes, go to TAP-021.
If no, go to step 79.

79 Retrieve conditions on the STS1 and STS3c paths associated with the VPL [DLP-100].

80 Check for BERP-LT, BERP-HT, or T-xxx conditions. Are any of these conditions present?

If yes, go to TAP-034.
If no, go to step 81.

81 Retrieve conditions on ATMPROC associated with the VPL [DLP-100].

82 Check for T-CDCONG0+1 conditions. Are any of these conditions present?

If yes, go to step 83.
If no, go to step 85.

83 ***NOTE:*** *A T-CDCONG0+1 condition indicates that congestion is occurring on the ATM Processor and cells are being discarded. There is insufficient bandwidth to handle all the ATM traffic.*

Consult office records and traffic engineering to determine action to take. (Also see TAP-052.)

84 STOP. This procedure is complete.

85 Have you retrieved alarms for any upstream NEs?

If yes, go to step 86.
If no, return to step 77, but this time retrieve alarms at first upstream NE.

86 Have you retrieved alarms for all upstream NEs?

If yes, go to step 87.
If no, return to step 77 and this time retrieve alarms at next upstream NE.

87 Contact Customer Service.

88 STOP. This procedure is complete.

TAP-054 Clear VCL Alarm

Purpose

Provides procedures for clearing Virtual Channel Link (VCL) alarms.

General

This procedure assumes that you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Have alarms and conditions been retrieved? If yes, go to step 3. If no, go to step 2.
2	Retrieve VCL alarms and conditions [DLP-100].
3	Locate the alarm or condition in Table A; the go to step indicated to clear it.

Table A. Alarms/Conditions/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
AIS	Alarm Indication Signal. VC AIS cells are being received because a failure occurred somewhere upstream.	4
INHCONTCE	Remote activation of VC connection continuity check has been inhibited.	6
INHCONTSE	Remote activation of VC segment continuity check has been inhibited.	8
INHPMCE	Remote activation of VC connection performance monitoring has been inhibited.	10
INHPMREPTCQOS	Reporting of scheduled VC connection PM reports has been inhibited.	12
INHPMREPTSQOS	Reporting of scheduled VC segment PM reports has been inhibited.	14
INHPMSE	VC segment performance monitoring has been inhibited.	16

Table A. Alarms/Conditions/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
LOSSCONTCE	Loss of VC Connection Continuity. The connection between the source NE and the sink NE may have been lost.	18
LOSSCONTSE	Loss of VC Segment Continuity. The connection between the segment endpoints may have been lost.	27
RFI	Remote Failure Indication. An LIF901 has detected a VC RDI. The VC RDI is generated by the far end NE at the other end of the VCL connection when it detects a VC AIS.	36
T-IMP0+1	Threshold violation for 0+1 impaired cell blocks	46
T-SECB	Threshold violation for severely errored cell blocks	46
T-TLOS0	Threshold violation for total lost 0 user information cells	46
T-TLOS0+1	Threshold violation for total lost 0+1 user information cells	46
Condition	**Description**	**Action**
ACTBKWDRPTCE	Backward reporting VP connection PM cells being received or transmitted	No action
ACTBKWDRPTSE	Backward reporting VP segment PM cells being received or transmitted	No action
ACTCONTCE	VC connection continuity cells being sourced or sinked	No action
ACTCONTSE	VC segment continuity cells being sourced or sinked	No action
ACTFWDMONCE	Forward monitoring VC connection PM cells being received or transmitted	No action
ACTFWDMONSE	Forward monitoring VC segment PM cells being received or transmitted	No action
AIS	VC AIS	No action
AISLOC	VC AIS defection location displayed as comment	No action
RDILOC	VC RDI defect location displayed as comment	No action

Table A. Alarms/Conditions/Events (cont)

Event	Description	Action
ACTBKWDRPTCE	Backward reporting VP connection PM cells being received or transmitted	No action
ACTBKWDRPTSE	Backward reporting VP segment PM cells being received or transmitted	No action
ACTCONTCE	VC connection continuity cells being sourced or sinked	No action
ACTCONTSE	VC segment continuity cells being sourced or sinked	No action
ACTFWDMONCE	Forward monitoring VC connection PM cells being received or transmitted	No action
ACTFWDMONSE	Forward monitoring VC segment PM cells being received or transmitted	No action

Alarm/Condition – AIS

NOTE: *A failure occurring somewhere upstream has been detected on a drop group VCL. Failures that trigger a VC AIS insertion are detected at VP connection endpoints or VC segment endpoints. The types of NEs that support these endpoints are typically ATM switches.*

4 Start troubleshooting a VC AIS at the NE where the VP connection endpoint (VPCE) or VC segment endpoint (VCSE) is setup in the downstream direction of traffic. (See Figure 1.)

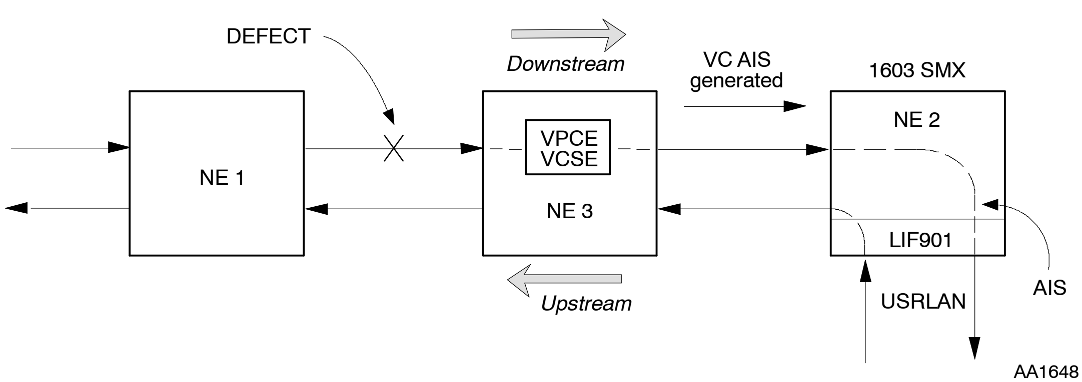


Figure 1. VC AIS Defect Flow

5 STOP. This procedure is complete.

Alarm/Condition – INHCONTCE

6 To clear alarm, allow remote activation of VC connection continuity check [DLP-555].

7 STOP. This procedure is complete.

Alarm/Condition – INHCONTSE

8 To clear alarm, allow remote activation of VC segment continuity check [DLP-555].

9 STOP. This procedure is complete.

Alarm/Condition – INHPMCE

10 To clear alarm, allow remote activation of VC connection performance monitoring [DLP-556].

11 STOP. This procedure is complete.

Alarm/Condition – INHPMREPTCQOS

12 To clear alarm, allow reporting of scheduled VC connection PM reports [DLP-510].

13 STOP. This procedure is complete.

Alarm/Condition – INHPMREPTSQOS

14 To clear alarm, allow reporting of scheduled VC segment PM reports [DLP-510].

15 STOP. This procedure is complete.

Alarm/Condition – INHPMSE

16 To clear alarm, allow remote activation of VC segment performance monitoring [DLP-556].

17 STOP. This procedure is complete.

Alarm/Condition – LOSSCONTCE

NOTE: *The NE reporting this alarm has been designated as a sink for an ATM connection continuity check. (See Figure 2.) A LOSSCONTCE alarm indicates that the connection between the source NE and the sink NE may have been lost. (Both the source NE and the sink NE must be connection endpoints.)*

NOTE: *There are several reasons why the connection may have been lost: a failure may have occurred in the network; a problem may exist with the cross-connection provisioning; or the continuity check may not have been set up properly.*

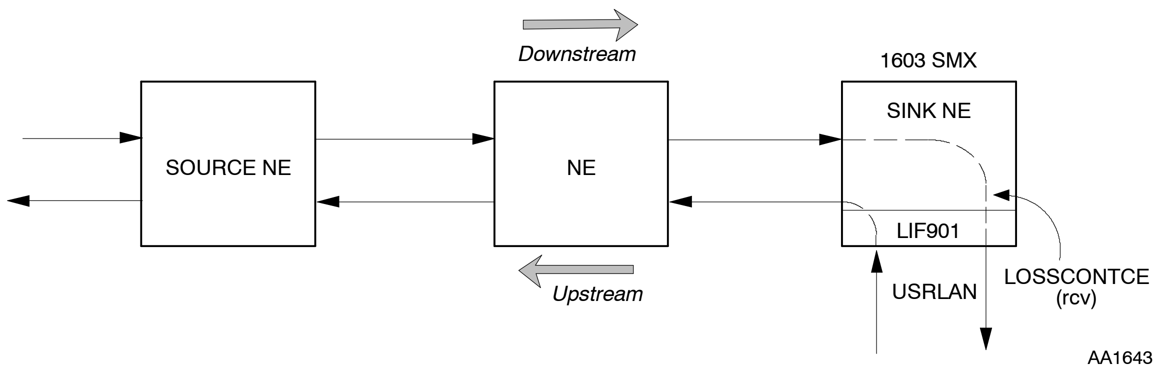


Figure 2. ATM Connection Continuity Check

18 Retrieve VCL conditions at the local (sink) NE [DLP-100].

19 Is there an AIS condition on this VCL?

If yes, go to step 4.
If no, go to step 20.

20 Retrieve alarms at the local (sink) NE [DLP-100].

21 Is there an LCD being reported on the ATM Port associated with this VCL?

If yes, go to TAP-051.
If no, go to step 22.

22 Retrieve VPL conditions at local NE [DLP-100].

23 Is there a VPL AIS condition being reported on the VPL associated with this VCL?

If yes, go to TAP-053.
If no, go to step 24.

24 Retrieve VCL conditions at the continuity source NE [DLP-100].

25 Is ACTCONTCE being reported for this VCL?

If yes, verify continuity setup.
If no, reactivate continuity setup.

26 STOP. This procedure is complete.

Alarm/Condition – LOSSCONTSE

NOTE: *The NE reporting this alarm has been designated as a sink for an ATM segment continuity check. (See Figure 3.) An LOSSCONTSE alarm indicates that the connection between the source NE and the sink NE may have been lost (Both the source NE and the sink NE must be segment endpoints.)*

NOTE: *There are several reasons why the connection may have been lost: a failure may have occurred in the network; a problem may exist with the cross-connection provisioning; or the continuity check may not have been set up properly.*

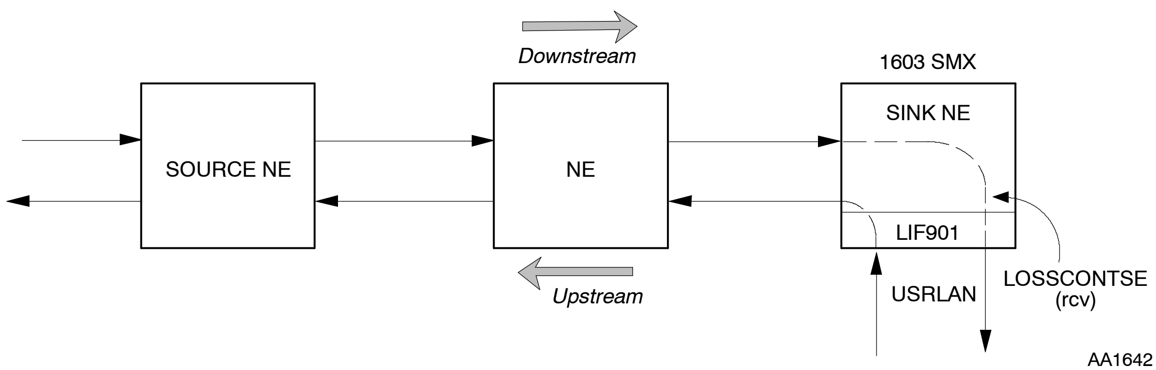


Figure 3. ATM Segment Continuity Check

27 Retrieve VCL conditions at the local (sink) NE [DLP-100].

28 Is there an AIS alarm condition on this VCL?

If yes, go to step 4.
If no, go to step 29.

29 Retrieve alarms at the local (sink) NE [DLP-100].

30 Is there an LCD being reported on the ATM Port associated with this VCL?

If yes, go to TAP-051.
If no, go to step 31.

31 Retrieve VPL conditions at local NE [DLP-100].

32 Is a VPL AIS condition being reported on the VPL associated with for this VCL?

If yes, go to TAP-053.
If no, go to step 33.

33 Retrieve VCL conditions at the VCL continuity source NE [DLP-100].

34 Is ACTCONTSE being reported for this VCL?

If yes, verify continuity setup.
If no, reactivate continuity setup.

35 STOP. This procedure is complete.

Alarm/Condition – RFI

NOTE: *An RFI alarm is generated when a VC RDI is detected on an LIF901. The VC RDI is generated by the far end NE at the other end of the VCL connection when it detects a VP AIS.*

NOTE: *In Figure 4, which depicts a VC RFI alarm, the VP connection endpoint and the VC connection endpoint are on the same NE. This is the case if the NE is a 1603 SM, SMX, or SE; however, if another ATM switching product is used, it is possible for the VP and VC connection endpoints to be at different points in the network.*

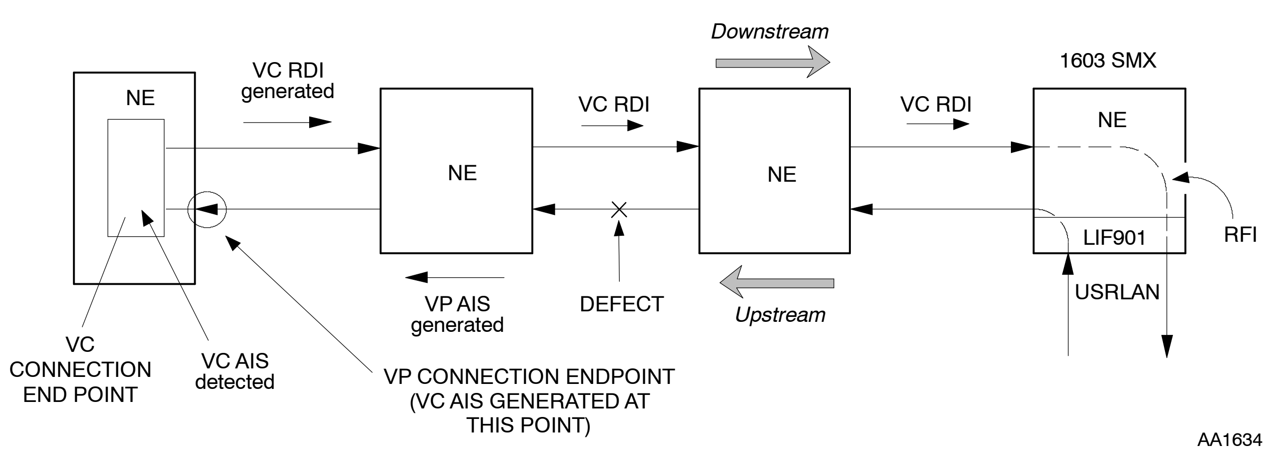


Figure 4. VCL RFI Alarm

36 Begin troubleshooting at the first NE that is upstream from the NE reporting the RFI alarm. (See Figure 4.)

37 Retrieve alarms at the first upstream NE [DLP-100].

38 Is the upstream NE reporting an LCD alarm in the upstream direction on any ATM Port associated with this VCL?

If yes, go to TAP-051.
If no, go to step 39.

39 Is the upstream NE reporting a VPL LOSSCONTSE alarm or LOSSCONTCE (in the upstream direction) for the VPL associated with this VCL?

If yes, go to TAP-053.
If no, go to step 40.

40 Retrieve alarms at the next upstream NE [DLP-100].

41 Is this NE reporting an LCD alarm in the upstream direction on any ATM Port associated with this VCL?

If yes, go to TAP-051.
If no, go to step 42.

42 Is this NE reporting a VPL LOSSCONTSE alarm or LOSSCONTCE (in the upstream direction) for the VPL associated with this VCL?

If yes, go to TAP-053.
If no, go to step 43.

43 Have you retrieved alarms for the NE with the VCL connection endpoint?

If yes, go to step 44.
If no, return to step 40.

44 Contact Customer Service.

45 STOP. This procedure is complete.

Alarm/Condition – T-IMP0+1, T-SECB, T-TLOS0, or T-TLOS0+1

NOTE: *These performance parameters, which are accumulated at an LIF901, are collected to determine Quality-of-Service (QOS). Data is collected over blocks of ATM data cells between two points in the network: segment endpoints and connection endpoints. An alarm is generated when a specified threshold value is exceeded.*

46 Retrieve alarms [DLP-100].

47 On Alarm Surveillance work view, select (highlight) threshold alarm and select Details button to display Alarm Details screen.

48 On the Alarm Details screen, note location of T-xxx alarm.

49 Find location of alarm in Table B, and take appropriate action to clear the threshold alarm.

Table B. Location of T-xxx Alarms

	LOCATION	DESCRIPTION	ACTION TO TAKE
1*	NEND	Errors detected on VCL data received at local NE	Perform steps 50–61 to analyze failure in downstream direction. (See Figure 5.)
2*	FEND	Errors detected on VCL data received at remote NE and reported back to local NE	Perform steps 50–61 to analyze failure in upstream direction. (See Figure 5.)
* *This number refers to the location where errors are detected as shown in in Figure 5.*			

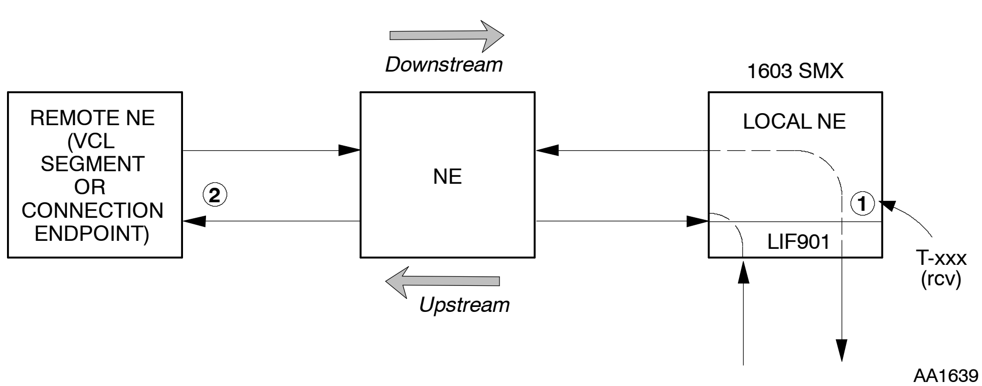


Figure 5. Receive NEND and FEND T-xxx on LIF901

50 Retrieve alarms at the local NE and check for equipment or SYNC alarms [DLP-100].

51 Are there any equipment or SYNC alarms?

If equipment alarms, go to TAP-021.
If SNYC alarms, go to TAP-027.
If no equipment or SYNC alarms, go to step 52.

52 Retrieve conditions on the STS1 and STS3c paths associated with the VPL [DLP-100].

53 Check for BERP-LT, BERP-HT, or T-xxx conditions. Are any of these conditions present?

If yes, go to TAP-034.
If no, go to step 54.

54 Retrieve conditions on ATMPROC associated with the VCL [DLP-100].

55 Check for T-CDCONG0+1 conditions. Are any of these conditions present?

If yes, go to step 56.
If no, go to step 58.

56 ***NOTE:*** *A T-CDCONG0+1 condition indicates that congestion is occurring on the ATM Processor and cells are being discarded. There is insufficient bandwidth to handle all the ATM traffic.*

Consult office records and traffic engineering to determine action to take. (Also see TAP-052.)

57 STOP. This procedure is complete.

58 Have you retrieved alarms for any upstream NEs?

If yes, go to step 59.
If no, return to step 50, but this time retrieve alarms at first upstream NE.

59 Have you retrieved alarms for all upstream NEs?

If yes, go to step 60.
If no, return to step 50, but this time retrieve alarms at next upstream NE.

60 Contact Customer Service.

61 STOP. This procedure is complete.

TAP-055
Clear AAL5 Alarm

Purpose

Provides procedures for clearing AAL5 alarms.

General

This procedure assumes that you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Have alarms and conditions been retrieved? If yes, go to step 3. If no, go to step 2.
2	Retrieve AAL5 alarms and conditions [DLP-100]
3	Find the alarm and/or condition in Table A; then go to the step indicated to clear it.

Table A. Alarms/Conditions/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
INHPMREPTQOS	Reporting of scheduled QOS PM reports have been inhibited	4
T-DISAAL5FR	AAL5 frames discarded due to no buffer space have exceeded threshold.	6
T-DISRFCHDR	AAL5 frames discarded due to RFC-1483 header errors have exceeded threshold.	6
T-PTCOLERR	AAL5 protocol errors have exceeded threshold.	6
T-TXERR	AAL5 transfer errors have exceeded threshold.	6

Alarm/Condition – INHPMREPTQOS

4 To clear alarm, allow scheduled QOS performance monitoring reports [DLP-510].

5 STOP. This procedure is complete.

Alarm/Condition – T-xxx

6 Refer to Table B for the default threshold values; then go to the step indicated in Table C to clear the alarm.

Table B. AAL5 PM THreshold Levels

MONITOR TYPE	FACTORY DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
T-DISAAL5FR	12	48	1...4,294,967,295	Number of AAL5 frames discarded due to no buffer space
T-DISRFCHDR	4	18	1...4,294,967,295	Number of AAL5 frames discarded due to bad RFC-1483 header
T-PTCOLERR	3	288	1...4,294,967,295	Sum of protocol errors
T-TXERR	2	192	1...4,294,967,295	Sum of transfer errors

Table C. Clear Threshold Violation Alarms

IF THRESHOLD VIOLATION IS...	PROBABLE CAUSE IS...	GO TO...
T-DISAAL5FR	More ATM traffic is being received from the network than there is bandwidth available on the USRLAN (Ethernet) facility	Step 7
T-DISRFCHDR	RFC-1483 encapsulation problems. Could be caused by transport problems in the network or RFC-1483 provisioning	Step 13
T-PTCOLERR	AAL5 protocol problems. Could be caused by transport problems in the network or traffic setup at far-end AAL5 port*	Step 13
T-TXERR	Network transport problems. CRC-32 checksum could be bad or the length field is invalid.	Step 13

* *The Common Part Indicator (CPI) field should always be all zeroes. The largest Service Data Unit (SDU) corresponds to an Ethernet packet size of 1518 bytes.*

T-DISAAL5FR

7 Check bandwidth allocation on USRLAN port [DLP-557].

8 Is USRLAN port provisioned for a 10BaseT (10 Mbps) interface or a 100BaseTx (100 Mbps) interface?

If 10BaseT, go to step 9.
If 100BaseTx, close work view and go to step 11.

9 Allocate more bandwidth on USRLAN port [DLP-557].

NOTE: *If you change the USRLAN port to 100BaseTx, then all devices connected to USRLAN may also have to be modified to operate at 100 Mbps.*

10 Did allocating more bandwidth on USRLAN port clear problem?

If yes, go to step 12.
If no, go to step 11.

11 Have traffic engineering reduce the amount of traffic being sent to this port.

12 STOP. This procedure is complete.

T-DISRFCHDR, T-PTCOLERR, or T-TXERR

13 Retrieve ATM Port conditions [DLP-100].

14 Are there any ATM Port conditions?

If yes, go to TAP-051.
If no, go to step 15.

15 Check for equipment or SYNC alarms [DLP-100].

16 Are there any equipment or SYNC alarms?

If equipment alarms, go to TAP-021 and clear alarms.
If SYNC alarms, go to TAP-027 and clear alarms.
If no equipment or SYNC alarms, go to step 17.

17 Retrieve alarms and conditions on the STS1 and STS3c paths [DLP-100].

18 Do any of the following conditions exist: BERP-LT, BERP-HT, or T-xxx?

If yes, go to TAP-034.
If no, go to step 19.

19 What type of condition are you trying to clear?

If T-DISRFCHDR, go to step 20.
If T-PTCOLERR, go to step 26.
If T-TXERR, contact Customer Service.

20 Check provisioning of ATM cell encapsulation [DLP-559].

21 Is encapsulation provisioned correctly (i.e., Off or RFC1483)?

If yes, go to step 24.
If no, go to step 22.

22 Change encapsulation provisioning [DLP-559].

23 Did changing encapsulation clear alarm?

If yes, go to step 25.
If no, go to step 24.

24 Check far end (of VC) AAL5 provisioning for RFC-1483.

25 STOP. This procedure is complete.

26 Check far end (of VC) AAL5 port setup.

27 If AAL5 port setup is okay, contact Customer Service.

28 STOP. This procedure is complete.

TAP-056
Clear USRLAN Alarm (LIF901)

Purpose

Provides procedures for clearing USRLAN alarms.

General

This procedure assumes that you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Have alarms and conditions been retrieved? If yes, go to step 3. If no, go to step 2.
2	Retrieve USRLAN alarms and conditions [DLP-100].
3	Identify the alarm and/or condition, then go to the step indicated in Table A to clear alarm.

Table A. Alarms/Conditions/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
INHPMREPTNDC	Reporting of scheduled NDC PM reports has been inhibited	4
INHPMREPTQOS	Reporting of scheduled QOS PM reports has been inhibited	6
LOS	Loss of Signal	8
MTCE	Removed from service for maintenance	15
T-CSERR	Carrier sense errors TCA*	17
T-DISFR	The traffic specification for the VPL associated with the USRLAN interface has been exceeded and USRLAN frames are being discarded because no buffer is available.	17
T-EXCOL	Excessive transmit collisions TCA*	17

Table A. Alarms/Conditions/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
T-FRCRC	Number of received frames with bad FCS TCA*	17
T-LFR	Number of received frames longer than maximum TCA*	17
T-LFRCOL	Number of late transmit collisions TCA*	17
Condition	**Description**	**Action**
AINS	Automatic In-Service state	No action
Event	**Description**	**Action**
AINS	Automatic In-Service state	No action
IS-AUTO	Automatic OOS-MA to IS	No action
* *Threshold Crossing Alert*		

Alarm/Condition – INHPMREPTNDC

4 To clear alarm, allow scheduled NDC performance monitoring reports [DLP-510].

5 STOP. This procedure is complete.

Alarm/Condition – INHPMREPTQOS

6 To clear alarm, allow scheduled QOS performance monitoring reports [DLP-510].

7 STOP. This procedure is complete.

Alarm/Condition - LOS

8 Check Ethernet cable on front of LIF901 and check connection to local equipment.

9 If cable connections are okay, ensure that USRLAN port is provisioned correctly for 100 Mbps vs 10 Mbps operation [DLP-557].

10 Is USRLAN port provisioned correctly?

If yes, close dialog and go to step 13.
If no, go to step 11.

11 Change provisioning of USRLAN port [DLP-557].

NOTE: *If you change the USRLAN port to 100BaseTx, then all devices connected to USRLAN may also have to be modified to operate at 100 Mbps.*

12 Did changing provisioning of USRLAN port clear problem?

If yes, go to step 14.
If no, go to step 13.

13 Contact Customer Service.

14 STOP. This procedure is complete.

Alarm/Condition - MTCE

15 To clear alarm, restore the USRLAN facility to in-service [DLP-501].

16 STOP. This procedure is complete.

Alarm/Condition – T-xxx

17 Refer to Table B for the default threshold values; then go to step indicated in Table C to clear alarm.

Table B. USRLAN PM Threshold Levels

MONITOR TYPE	FACTORY DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
CSERR	24	2304	1...4,294,967,295	Carrier sense errors
DISFR	40	3840	1...4,294,967,295	Number of received frames discarded due to no buffer available
EXCOL	24	2304	1...4,294,967,295	Excessive collisions
FRCRC	4	384	1...4,294,967,295	Number of received frames with bad FCS (CRC errors)
LFR	8	768	1...4,294,967,295	Number of received frames longer than the maximum length
LFRCOL	24	2304	1...4,294,967,295	Multiple collision frames

Table C. Clear Threshold Violation Alarms

IF THRESHOLD VIOLATION IS...	PROBABLE CAUSE IS...	GO TO...
T-CSERR	Ethernet connectivity problems	Step 18
T-DISFR (rcv)	More Ethernet frames are being retrieved than there is bandwidth allocated for entry into the network	Step 25
T-EXCOL (trmt)	Overloaded Ethernet hub/router or Ethernet connectivity problems	Step 28
T-FRCRC (rcv)	Ethernet connectivity problems	Step 18
T-LFR (rcv)	Ethernet connectivity problems or equipment sourcing the Ethernet traffic could be setup improperly. (Maximum frame size allowed is 1518 bytes.)	Step 39
T-LFRCOL (trmt)	Overloaded Ethernet hub/router or Ethernet connectivity problems	Step 28

T-CSERR and T-FRCRC

18 Check Ethernet cable connection on front of LIF901 and check connection to local equipment.

19 If cable connections are okay, ensure that USRLAN port is provisioned correctly for 100 Mbps vs 10 Mbps operation [DLP-557].

20 Is USRLAN port provisioned correctly?

If no, go to step 21.
If yes, close work view and go to step 23.

21 Change provisioning of USRLAN port [DLP-557].

NOTE: *If you change the USRLAN port to 100BaseTx, then all devices connected to USRLAN may also have to be modified to operate at 100 Mbps.*

22 Did changing provisioning of USRLAN port clear problem?

If yes, go to step 24.
If no, go to step 23.

23 Contact Customer Service.

24 STOP. This procedure is complete.

T-DISFR

25 ***NOTE:*** *The policing that generated this threshold alarm may be acceptable under certain situations, for example, during peak traffic conditions. However, if thresholds are being exceeded during non-peak conditions, traffic descriptor characteristics for this VPL may be set too low.*

Do you want to change traffic descriptor characteristics?

If yes, go to step 26.
If no, go to step 27.

26 Change traffic descriptor characteristics [DLP-530].

27 STOP. This procedure is complete.

T-EXCOL and T-LFRCOL

28 Check Ethernet cable on front of LIF901 and check connection to local equipment.

29 If cable connections are okay, ensure that USRLAN port is provisioned correctly for 100 Mbps vs 10 Mbps operation [DLP-557].

30 Is USRLAN port provisioned correctly?

If yes, close work view and go to step 35.
If no, go to step 31.

31 Change provisioning of USRLAN port [DLP-557].

NOTE: *If you change the USRLAN port to 100BaseTx, then all devices connected to USRLAN may also have to be modified to operate at 100 Mbps.*

32 Did changing provisioning of USRLAN port clear problem?

If yes, STOP. This procedure is complete.
If no, go to step 33.

33 Contact Customer Service.

34 STOP. This procedure is complete.

35 Try reducing traffic load at Ethernet hub/router by either using another hub/router or have traffic engineering reduce traffic from the network.

36 Did reducing traffic clear problem?

If yes, STOP. This procedure is complete.
If no, go to step 37.

37 Contact Customer Service.

38 STOP. This procedure is complete.

T-LFR

39 Check Ethernet cable on front of LIF901 and also check connection to local equipment.

40 If cable connections are okay, ensure that USRLAN port is provisioned correctly for 100 Mbps vs 10 Mbps operation [DLP-557].

41 Is USRLAN port provisioned correctly?

If yes, close work view and go to step 44.
If no, go to step 42.

42 Change provisioning of USRLAN port [DLP-557].

NOTE: *If you change the USRLAN port to 100BaseTx, then all devices connected to USRLAN may also have to be modified to operate at 100 Mbps.*

43 Did changing provisioning of USRLAN port clear problem?

If yes, STOP. This procedure is complete.
If no, go to step 44.

44 Check Ethernet setup at the source of the Ethernet traffic. Correct if necessary.

45 Were changes made to the setup?

If yes, go to step 46.
If no, go to step 47.

46 Did changes clear alarm?

If yes, go to step 48.
If no, go to step 47.

47 Contact Customer Service.

48 STOP. This procedure is complete.

TAP-057
Clear USRLAN Alarm (LIFG01)

Purpose

Provides procedures for clearing USRLAN alarms generated by an LIFG01 unit.

General

This procedure assumes that you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Have alarms and conditions been retrieved? If yes, go to step 3. If no, go to step 2.
2	Retrieve USRLAN alarms and conditions [DLP-100].
3	Identify the alarm and/or condition, then go to the step indicated in Table A to clear alarm.

Table A. Alarms/Conditions/Events

ALARM/CONDITION	**REASON FOR ALARM**	**STEP**
INHPMREPTNDC	Reporting of scheduled Network Data Collection (NDC) PM reports has been inhibited	4
INHPMREPTQOS	Reporting of scheduled Quality of Service (QOS) PM reports has been inhibited	6
LINENA	Line Not Available. Possible reasons for alarm: an invalid code error, a 10 bit sync error, or a port link test failed.	8
LOS	Loss of Signal	14
LPR	Low laser light	20
MTCE	Removed from service for maintenance	29
T-DISFR	The number of frames being discarded because no buffer is available has exceeded the threshold*	31
T-EXCOL	An excessive number of transmit collisions has occurred and the threshold has been exceeded*	31
T-FRCRC	The number of received frames with bad FCS (CRC errors) has exceeded the threshold*	31
T-LFR	The number of frames received that are longer than the allowed maximum length has exceeded the threshold*	31
T-LFRCOL	The number of late transmit collisions has exceeded the threshold*	31
T-SFR	The number of frames received that are shorter than the allowed minimum length has exceeded the threshold*	31
Condition	**Description**	**Action**
AINS	Automatic In-Service state	No action
Event	**Description**	**Action**
AINS	Automatic In-Service state	No action
IS-AUTO	Automatic OOS-MA to IS	No action
* *Threshold Crossing Alert*		

Alarm/Condition – INHPMREPTNDC

4 To clear alarm, allow scheduled NDC performance monitoring reports [DLP-510].

5 STOP. This procedure is complete.

Alarm/Condition – INHPMREPTQOS

6 To clear alarm, allow scheduled QOS performance monitoring reports [DLP-510].

7 STOP. This procedure is complete.

Alarm/Condition - LINENA

8 Check condition of fiber optic cable.

9 Check the cable connection at the LIFG01 unit. (May require doing Auto Negotiation)

10 If the condition of the fiber and the connection are okay, replace the LIFG01 unit [DLP-101].

11 Did replacing the unit clear the alarm?

If yes, go to step 13.
If no, then go to step 12.

12 Contact Customer Service.

13 STOP. This procedure is complete.

Alarm/Condition - LOS

14 Check condition of fiber optic cable.

15 Check cable connection at the LIFG01 unit.

16 If cable connections are okay, ensure that the far end Physical Layer is provisioned for 1 Gigabit operation (1000BASELX) and the Duplex Mode is provisioned for Full Duplex.

NOTE: *All devices connected to USRLAN must also operate at 1 Gigabit.*

17 Did USRLAN facility clear problem?

If yes, go to step 19.
If no, go to step 18.

18 Contact Customer Service.

19 STOP. This procedure is complete.

Alarm/Condition - LPR

20 At the near-end NE, check optic level of received signal.

21 Is the received optic level within range?

If yes, go to step 22.
If no, then go to step 25.

22 Replace the LIFG01 unit [DLP-101].

23 Retrieve alarms [DLP-100].

24 Did alarm clear?

If yes, go to step 28.
If no, then go to step 27.

25 Perform transmission test on the fiber per local procedure.

26 Did transmission test pass?

If yes, go to step 27.
If no, correct transmission problem.

27 Contact Customer Service.

28 STOP. This procedure is complete.

Alarm/Condition - MTCE

29 To clear alarm, restore the USRLAN facility to in-service [DLP-501].

30 STOP. This procedure is complete.

31 Refer to Table B for the default threshold values; then go to step indicated in Table C to clear alarm.

Table B. USRLAN PM Threshold Levels

MONITOR TYPE	FACTORY DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
DISFR	40	3840	1...4,294,967,295	Number of received frames discarded due to no buffer available
EXCOL	24	2304	1...4,294,967,295	Number of excessive collisions
FRCRC	4	384	1...4,294,967,295	Number of received frames with bad Frame Check Sequence (FCS) (CRC errors)
LFR	8	768	1...4,294,967,295	Number of frames being received by the USRLAN interface that are longer than the maximum length
LFRCOL	24	2304	1...4,294,967,295	Number of late transmit collisions
SFR	8	768	1...4,294,967,295	Number of frames being received by USRLAN interface that are shorter than the required minimum length

Table C. Clear Threshold Violation Alarms

IF THRESHOLD VIOLATION IS...	PROBABLE CAUSE IS...	GO TO...
T-DISFR (rcv)	Not enough bandwidth is allocated for the number of Ethernet frames being received.	Step 32
T-EXCOL (trmt)	Overloaded Ethernet hub/router or Ethernet connectivity problems	Step 34
T-FRCRC (rcv)	Ethernet connectivity problems	Step 43
T-LFR (rcv)	Ethernet connectivity problems or equipment sourcing the Ethernet traffic is setup improperly.	Step 49

Table C. Clear Threshold Violation Alarms(cont)

IF THRESHOLD VIOLATION IS...	PROBABLE CAUSE IS...	GO TO...
T-LFRCOL (trmt)	Overloaded Ethernet hub/router or Ethernet connectivity problems	Step 34
T-SFR (rcv)	Ethernet connectivity problems or equipment sourcing the Ethernet traffic is setup improperly.	Step 49

T-DISFR

32 ***NOTE:*** *Ethernet frames are being received faster than they can be buffered.*

Have traffic engineering reduce Gigabit Ethernet traffic from the network.

33 STOP. This procedure is complete.

T-EXCOL and T-LFRCOL

34 Check fiber optic cable on front of LIFG01 and check connection to local equipment.

35 If cable connections are okay, ensure that the far end Physical Layer is provisioned for 1 Gigabit operation (1000BASELX) and the Duplex Mode is provisioned for Full Duplex.

36 Wait several minutes; then retrieve USRLAN PM registers [DLP-517] and note EXCOL and LFRCOL counts.

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

37 Have USRLAN facility PM counts been reduced?

If yes, STOP. This procedure is complete.
If no, go to step 38.

38 Try reducing traffic load at Ethernet hub/router by either using another hub/router or have traffic engineering reduce traffic from the network.

39 Wait several minutes; then retrieve USRLAN PM registers [DLP-517] and note EXCOL and LFRCOL counts.

40 Did reducing traffic reduce PM counts?

If yes, go to step 42.
If no, go to step 41.

41 Contact Customer Service.

42 STOP. This procedure is complete.

T-FRCRC

43 Check fiber optic cable connection on front of LIFG01 and check connection to local equipment.

44 If cable connections are okay, ensure that the far end Physical Layer is provisioned for 1 Gb operation (1000BASELX) and the Duplex Mode is provisioned for Full Duplex.

45 Wait several minutes; then retrieve USRLAN PM registers [DLP-517] and note FRCRC counts.

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

46 Have USRLAN facility FRCRC PM counts been reduced?

If yes, go to step 48.
If no, go to step 47.

47 Contact Customer Service.

48 STOP. This procedure is complete.

T-LFR and T-SFR

49 Check fiber optic cable on front of LIFG01 and also check connection to local equipment.

50 If cable connections are okay, ensure that the far end Physical Layer is provisioned for 1 Gb operation (1000BASELX) and the Duplex Mode is provisioned for Full Duplex.

51 Wait several minutes; then retrieve USRLAN PM registers [DLP-517] and note LFR and SFR counts.

NOTE: *The value provisioned in the Refresh Rate field dictates how frequently the 1301 NMX retrieves new register values.*

52 Have USRLAN PM counts been reduced?

If yes, STOP. This procedure is complete.
If no, go to step 53.

53 Contact Customer Service.

TAP-058
Clear BLSR Alarm

Purpose

Provides procedures for clearing BLSR alarms.

General

This procedure assumes that you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Have alarms and conditions been retrieved? If yes, go to step 3. If no, go to step 2.
2	Retrieve BLSR alarms and conditions [DLP-100].
3	Identify the alarm and/or condition, then go to the step indicated in Table A to clear alarm.

Table A. Alarms/Conditions/Events

ALARM/CONDITION	REASON FOR ALARM	STEP
BLSRCONN-LG1	Inter-node connectivity lost in 2 Fiber BLSR to NE on LG1	4
BLSRCONN-LG2	Inter-node connectivity lost in 2 Fiber BLSR to NE on LG2	4
BLSRMULTIFLT	There are two or more ring faults that are causing BLSR node(s) to be isolated from this BLSR node. This alarm is only generated on nodes that are in the BLSR switching state.	11
BLSRPROV-LG1	NE on LG1 does not have BLSR Mode or Automatic Map Generation provisioned correctly.	15
BLSRPROV-LG2	NE on LG2 does not have BLSR Mode or Automatic Map Generation provisioned correctly.	15
BLSROUTOFSYNC	BLSR cross-connections, sequence maps and/or squelch tables on NEs around the BLSR ring are not up to date.	24

Table A. Alarms/Conditions/Events (cont)

ALARM/CONDITION	REASON FOR ALARM	STEP
DUPNODEID	A duplicate node ID exists in BLSR ring map.	26
RINGBLSRALM	A severity bridge request exists somewhere on the ring. This alarm is valid in both BLSR switching and pass through states.	33
RINGMAPPROV	A BLSR sequence map is misprovisioned.	38
RINGXCONNPROV	A cross connect is misprovisioned on the BLSR ring.	44
Condition	**Description**	**Action**
KSTATE	K byte state (command only)	No Action
KSTATE-IDLE	K byte state idle (response only)	No Action
KSTATE-SWITCHING	K byte state switching (response only)	No Action
KSTATE-PASSTHRU-UNI	K byte state Passthru Unidirectional Full (response only)	No Action
KSTATE-PASSTHRU-BI	K byte state Passthru Bidirectional Full (response only)	No Action
KSTATE-PASSTHRU-KBYTE	K byte state Passthru Kbyte (response only)	No Action
LG1SWPRIORITY	LG1 switch priority (NEND/FEND) (command only)	No Action
LG1SWPRIORITY - yyy*	LG1 switch priority (NEND/FEND) (response only)	No Action
LG2SWPRIORITY	LG2 switch priority (NEND/FEND) (command only)	No Action
LG2SWPRIORITY - yyy*	LG2 switch priority (NEND/FEND) (command only)	No Action
* *yyy = IDLE (idle), WTR (wait to restore), MAN (wait to restore), SIGDEG (signal degraded), SIGFAIL (signal failed), FRCD (force switch request), LPS (lockout – entire ring), or LOWR (lockout – local NE).*		

Alarm/Condition – BLSRCONN (LG1 or LG2)

4 Check the fiber connections between NEs.

5 Are connections OK?

If yes, go to step 7.
If no, reconnect fiber.

6 STOP. This procedure is complete.

7 Are there any equipment alarms [DLP-100]?

If yes, go to TAP-021.
If no, go to step 8.

8 Are there any OC48 facility alarms [DLP-100]?

If yes, go to TAP-029.
If no, go to step 9.

9 Are there any DCC-Lower Layer alarms [DLP-100]?

If yes, go to TAP-032.
If no, contact Customer Service.

10 STOP. This procedure is complete.

Alarm/Condition – BLSRMULTIFLT

11 Are there any other BLSR alarms [DLP-100]?

If yes, go to step 3.
If no, go to step 12.

12 Are there any OC48 facility alarms [DLP-100]?

If yes, go to TAP-029 and clear OC48 facility alarms.
If no, go to step 13.

13 Contact Customer Service.

14 STOP. This procedure is complete.

Alarm/Condition – BLSRPROV (LG1 or LG2)

15 On the NE on LG1 side, retrieve BLSR Ring parameters and check provisioning of BLSR Mode and Automatic Map Generation parameters [DLP-543].

16 Are BLSR Mode and Automatic Map Generation parameters provisioned the same?

If yes, go to step 17.
If no, go to step 19.

17 On the NE on LG2 side, check provisioning of BLSR Mode and Automatic Map Generation parameters [DLP-543].

18 Are BLSR Mode and Automatic Map Generation parameters provisioned the same?

If yes, go to step 22.
If no, go to step 19.

19 Change the provisioning so the BLSR Mode and Automatic Map Generation are the same on both NEs [DLP-543].

20 Check for BLSR alarms [DLP-100].

21 Did alarm clear?

If yes, go to step 23.
If no, go to step 22.

22 Contact Customer Service.

23 STOP. This procedure is complete.

Alarm/Condition – BLSROUTOFSYNC

24 Warm start NEP on local NE and on neighboring NEPs [DLP-554].

25 STOP. This procedure is complete.

Alarm/Condition – DUPNODEID

26 Retrieve BLSR Automatic Sequence Map and check for duplicate node IDs on the BLSR ring [DLP-564].

27 Were any duplicate node IDs found?

If yes, go to step 28.
If no, go to step 30.

28 Select one of the NEs with a duplicate node ID, log on to that NE and change the Node ID [DLP-543].

29 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 30.

30 Contact Customer Service.

31 STOP. This procedure is complete.

Alarm/Condition – RINGBLSRALM

32 Retrieve alarms [DLP-100].

33 Are there any other BLSR alarms?

If yes, go to step 3 and clear these alarm.
If no, go to step 34.

34 Are there any OC48 facility alarms?

If yes, go to TAP-029 and clear these alarms.
If no, go to step 35.

35 Are there any equipment alarms?

If yes, go to TAP-021.
If no, go to step 36.

36 Contact Customer Service.

37 STOP. This procedure is complete.

Alarm/Condition – RINGMAPPROV

38 Check provisioning of BLSR Manual Sequence Maps at each NE on the BLSR ring [DLP-563].

39 Were all sequence maps provisioned correctly?

If yes, go to step 42.
If no, go to step 40.

40 Change any Manual Sequence Maps that are not provisioned correctly [DLP-563].

41 STOP. This procedure is complete.

42 Contact Customer Service.

43 STOP. This procedure is complete.

Alarm/Condition – RINGXCONNPROV

44 Retrieve BLSR ring conditions [DLP-100].

45 On the Monitor Conditions screen, locate RINGXCONNPROV in the Condition column.

46 In the same row as RINGXCONNPROV, note the NE(s) listed in the Description column. These are the NEs that have misconnected cross-connections.

47 Log on to an NE in the list and reprovision the cross-connect [DLP-504].

48 Have cross-connections been changed for all NEs on the list?

If yes, go to step 49.
If no, return to step 47.

49 STOP. This procedure is complete.

TAP-059
Clear POS Port Alarm

Purpose

Provides procedures for clearing POS Port alarms.

General

This procedure assumes that you have logged on to the alarmed Network Element (NE) using the 1301 NMX Explorer and have opened the 1603 SMX Application browser [DLP-117].

Refer to TAP-001 for assistance in analyzing alarms and isolating alarms to specific NEs.

STEP	PROCEDURE
1	Have alarms and conditions been retrieved? If yes, go to step 3. If no, go to step 2.
2	Retrieve POS Port alarms and conditions [DLP-100].
3	Locate the alarm you want to clear in Table A; then go to step indicated to clear it.

Table A. Alarms/Conditions

ALARM/CONDITION	REASON FOR ALARM	STEP
INHPMREPTNDC	Reporting of scheduled Network Data Collection (NDC) PM reports has been inhibited	4
INHPMREPTQOS	Reporting of scheduled Quality of Service (QOS) PM reports has been inhibited	6
INVLDADRCTL	A POS packet is carrying an Invalid address control field	8
T-ABTPKT	The number of Abort Sequence Packets received has exceeded the threshold.*	17
T-DISFR	The number of frames being discarded because no buffer is available has exceeded the threshold.*	17
T-FCSERR	The number of HDLC Frames received with Bad Frame Check Sequence has exceeded the threshold.*	17
T-LPKT	The number of packets received that are longer than the allowed maximum length has exceeded the threshold.*	17
T-SPKT	The number of packets received that are shorter than the allowed minimum length has exceeded the threshold.*	17
* *Threshold Crossing Alert*		

Alarm/Condition – INHPMREPTNDC

4 To clear alarm, allow scheduled QOS reports [DLP-510].

5 STOP. This procedure is complete.

Alarm/Condition – INHPMREPTQOS

6 To clear alarm, allow scheduled QOS reports [DLP-510].

7 STOP. This procedure is complete.

Alarm/Condition – INVLDADRCTL

8 At the local NE, check for equipment or STS12c alarms [DLP-100].

9 Are any equipment or STS12c alarms being reported?

If equipment alarms, go to TAP-021.
If STS12c alarms, go to TAP-034.
If there are no equipment or STS12c alarms, go to step 10.

10 Check cross-connection for the STS12c path [DLP-504].

11 Is the cross-connection correct?

If yes, go to step 13.
If no, go to step 12.

12 Re-establish STS12c path cross-connect [DLP-504].

13 At the far-end NE where the POS cells are mapped onto the STS12c path, check for equipment or STS12c alarms [DLP-100].

14 Are any equipment or STS12c alarms being reported at the far-end NE?

If equipment alarms, go to TAP-021.
If STS12c alarms, go to TAP-034.
If there are no equipment or STS12c alarms, go to step 15.

15 Contact Customer Service.

16 STOP. This procedure is complete.

Alarm/Condition – T-ABTPKT, T-DISFR, T-FCSERR, T-LPKT, or T-SPKT

17 At the local NE, check for STS12c alarms [DLP-500].

18 Are any STS12c alarms being reported?

If yes, go to TAP1-034 to clear the alarm(s).
If no, then go to step 19.

19 Check cross-connection for the STS12c path [DLP-504].

20 Is the cross-connection correct?

If yes, go to step 24.
If no, then go to step 21.

21 Re-establish STS12c path cross-connect [DLP-504].

22 Did re-establishing cross-connect clear alarm?

If yes, go to step
If no, then go to step

23 Check for equipment or STS12c alarms at the far-end NE?

24 Are any equipment or STS12c alarms being reported?

If equipment alarms, go to TAP-021.
If STS12c alarms, go to TAP-034.
If there are no equipment or STS12c alarms, go to step 25.

25 ***NOTE:*** *A threshold exceeded alarm can be disabled by changing the threshold level.*

Do you want to change the threshold?

If yes, go to step 26.
If no, then go to step 28.

26 Change POS PM threshold level [DLP-574]. Refer to Table B for default threshold values.

27 STOP. This procedure is complete.

Table B. POS Port PM Threshold Levels

MONITOR TYPE	FACTORY DEFAULT		RANGE	DESCRIPTION
	15-MIN	1-DAY		
ABTPKT	20	1920	1...4,294,967,295	The number of received abort sequence packets
DISFR	40	3840	1...4,294,967,295	The number of frames being discarded because no buffer is available
FCSERR	20	1920	1...4,294,967,295	The number of HDLC frames received with bad Frame Check Sequence (FCS) (CRC errors)
LPKT	20	1920	1...4,294,967,295	The number of packets received that are longer than the maximum allowed length
SPKT	20	1920	1...4,294,967,295	The number of packets received that are shorter than the minimum allowed length

28 Contact Customer Service.

29 STOP. This procedure is complete.

DLP-012
Clean Fibers

Purpose

This procedure describes the standard practice to clean fibers.

STEP	PROCEDURE
1	**DANGER: Possibility of personal injury. Exercise caution when handling unterminated fibers. If far-end equipment is active, invisible laser radiation is present at the fiber ends. Avoid direct exposure to beam.**
2	Clean fibers per local practice. If no local practice exists, complete the following steps.
3	Spray connector end with Contact-Renu® or equivalent nonresidue cleaner.
4	Wipe ferrule end with a lint-free cloth or tissue such as Kim-wipe®.
5	Blow compressed air into the optical connectors (IN and OUT) on the HIF plug-in.
6	STOP. This procedure is complete.

DLP-016
Test OC3 Protection Switching

Purpose

This procedure describes how to test OC3 protection switching.

STEP	PROCEDURE

1 Determine the facility protection switching mode at both ends of the OC3 span:

a. In the scope pane, expand Facility and select OC3.

b. In the result pane, right-click OC3 facility being tested to display a context menu.

c. From the context menu, select **Task>Provision>Switch** to display a work view.

d. Verify parameters are provisioned per company requirements.

NOTE: *The switch direction parameter must be set to the same value (unidirectional or bidirectional) at both ends of the OC3 facility.*

e. If necessary, modify switching parameters.

f. On the toolbar, select Submit; then close work view.

2 Refer to Table A and select the test you want to perform; then go to the referenced step.

Table A. Protection Switching Choices

IF SWITCH DIRECTION IS...	AND YOU WANT TO PERFORM A...	THEN GO TO...
Unidirectional	Normal Switch	Step 3
	Fast Switch	Step 10
Bidirectional	Normal Switch	Step 19
	Fast Switch	Step 26

Unidirectional (Normal Switch)

3 Switch OC3 facility [DLP-515].

4 Verify the switch took place by observing ACT (active) LEDs on the HIF/LIF and Service Condition column.

5 Did switch take place?

If yes, go to step 7.
If no, then go to step 6.

6 Verify there are no alarms on the OC3 facility. If necessary, replace HIF/LIF plug-ins [DLP-101]; then repeat procedure.

7 Release facility protection switch [DLP-545].

NOTE: *If switching mode is revertive, facility returns to the A-side. If nonrevertive, facility does not return to A-side.*

8 Log on to the Network Element (NE) that terminates the OC3 span and repeat steps 3 through 7.

9 STOP. This procedure is complete.

Unidirectional (Fast Switch)

10 Allow fast facility protection (FFP) switch [DLP-573].

11 Switch OC3 facility [DLP-515].

12 Repeat switch (step 11) several times.

13 Retrieve PM registers [DLP-517] and verify that the PSC, Protection Switch Count, register recorded all the switches.

14 Did all the switches take place?

If yes, go to step 16.
If no, then go to step 15.

15 Verify there are no alarms on the OC3 facility. If necessary, replace HIF/LIF plug-ins [DLP-101]; then repeat procedure.

16 Release facility protection switch [DLP-545].

NOTE: *If switching mode is revertive, facility returns to the A-side. If nonrevertive, facility does not return to A-side.*

17 Log on to the Network Element (NE) that terminates the OC3 span and repeat steps 11 through 16.

18 STOP. This procedure is complete.

Bidirectional (Normal Switch)

19 ***NOTE:*** *Observe that switching takes place at both NEs.*

Log on to the NE that terminates the OC3 span [DLP-117] if a craftsperson is not there to observe events.

20 At one NE only, switch OC3 facility [DLP-515].

21 Verify the switch took place at both NEs by observing ACT (active) LEDs on the HIF/LIF and Service Condition column.

22 Did switch take place?

If yes, go to step 24
If no, then go to step 23.

23 Verify there are no alarms on the OC3 facility. If necessary, replace HIF/LIF plug-ins [DLP-101]; then repeat procedure.

24 Release facility protection switch [DLP-545].

NOTE: *If switching mode is revertive, facility returns to the A-side. If nonrevertive, facility does not return to A-side.*

25 STOP. This procedure is complete.

Bidirectional (Fast)

26 ***NOTE:*** *Observe that switching takes place at both NEs.*

Log on to the NE that terminates the OC3 span [DLP-117] if a craftsperson is not there to observe events.

27 Allow fast facility protection (FFP) switch [DLP-573].

28 At one NE only, switch OC3 facility [DLP-515].

29 Retrieve PM registers [DLP-517] at both NEs and verify that the PSC, Protection Switch Count, register recorded all the switches.

30 Did all the switches take place?

If yes, go to step 32.
If no, then go to step 31.

31 Verify there are no alarms on the OC3 facility. If necessary, replace HIF/LIF plug-ins [DLP-101]; then repeat procedure.

32 Release facility protection switch [DLP-545].

NOTE: *If switching mode is revertive, facility returns to the A-side. If nonrevertive, facility does not return to A-side.*

33 STOP. This procedure is complete.

DLP-019
Verify/Connect X.25 Port Wiring

Purpose

This procedure describes how to verify and connect X.25 port wiring.

STEP	PROCEDURE

NOTE: *A special cable stub is available from Alcatel (P/N 601363-540-018). This RS-232 cable is 18 inches long with unterminated wires on one end for wire-wrapping to the 1603 SMX backplane and a female DB-25 connector on the other end. The cable is wired per Table A.*

Table A. Craft 2 Port Interface Wiring for X.25 Port

1603 SMX BACKPLANE SIGNAL	BACKPLANE SIGNAL DIRECTION	DESCRIPTION	DB25 WIRING
DCD-T	--->	Carrier Detect (RLSD)	–
DSR-T	--->	Data Set Ready	20
CTS-T	--->	Clear To Send	4
RXD-T	--->	Receive Data	2
DTR-T	<---	Data Terminal Ready	6
RTS-T	<---	Request To Send	5
TXD-T	<---	Transmit Data	3
OPT-T	<---	RXD Clock (Required)	17
FG		Frame Ground	–
SG		Signal Ground	7

NOTE: *X.25 service is provided at the Craft 2 port through a synchronous modem, Data Service Unit (DSU) or a similar device. Such a device provides a DCE interface and generates the receive timing signal for the X.25 (Craft 2) port.*

NOTE: *The recommended connections to the 1603 SMX backplane (Figure 1) are detailed in Table A. The cable assembly wired per Table A can also be used to connect to a dial-up modem.*

1 Verify there are no straps (jumpers) between DTR-T, RTS-T and SG pins. Remove these straps if present.

2 STOP. This procedure is complete.

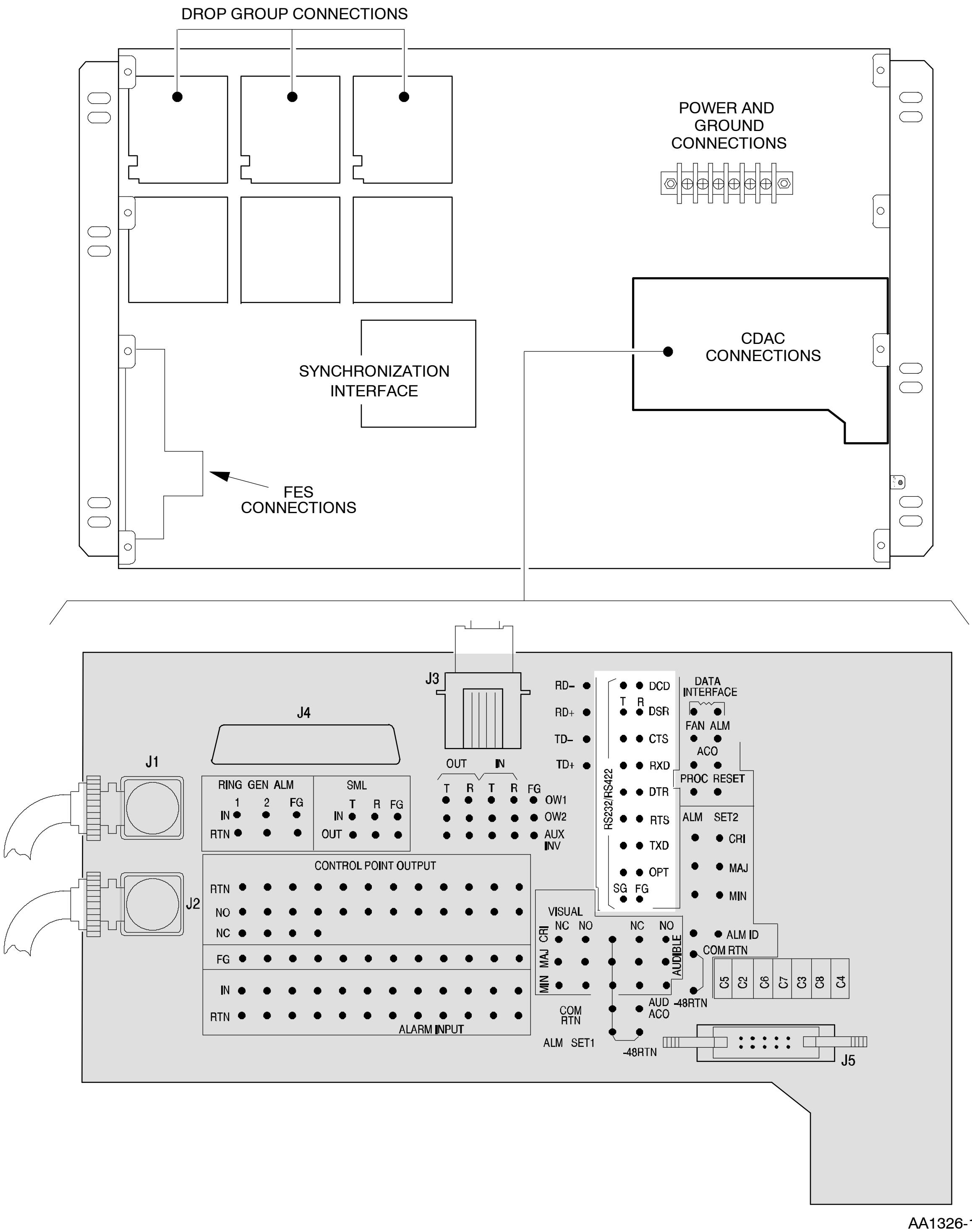


Figure 1. 1603 SMX Backplane and CDAC Layout

DLP-020
Verify/Connect LAN Wiring

Purpose

This procedure describes how to verify and connect LAN wiring.

STEP	PROCEDURE
1	***NOTE:*** *The 10Base2 requires RG 58 coaxial cable or equivalent and a 50-ohm terminator at both ends of the network. There is a maximum of 600 feet end-to-end cable restriction without a repeater.* ***NOTE:*** *The 10BaseT requires unshielded twisted pair 22 to 26 AWG using an RJ-45 male 8-pin connector. There is a maximum of 328 feet from the NE to hub (central control node) without a repeater.* Locate LAN wiring on shelf backplane (see Figure 1).
2	***NOTE:*** *Connections to a 10Base2 and a 10BaseT network may be simultaneously maintained; however, only one is operational (provisioned) at a time.* Per job documentation, determine if LAN connections are for 10Base2 (coax) or 10BaseT (twisted pair).
3	Is wiring for 10Base2 or 10BaseT? If 10Base2, go to step 4. If 10BaseT, go to step 8.
4	Run RG 58 coaxial cable (terminated with male BNC connectors) between the 1603 SMX shelves (see Figure 2).
5	Connect the coaxial cables on the 1603 SMX shelf on BNC connectors J1 or J2.
6	At the two shelves that terminate the bus, install 50-ohm termination (obtained locally) in the unused BNC connector.
7	STOP. This procedure is complete.
8	Run two unshielded twisted pair cables (terminated with RJ-45 8-pin connectors) between the 1603 SMX shelf and the hub (central control node) equipment (see Figure 3).

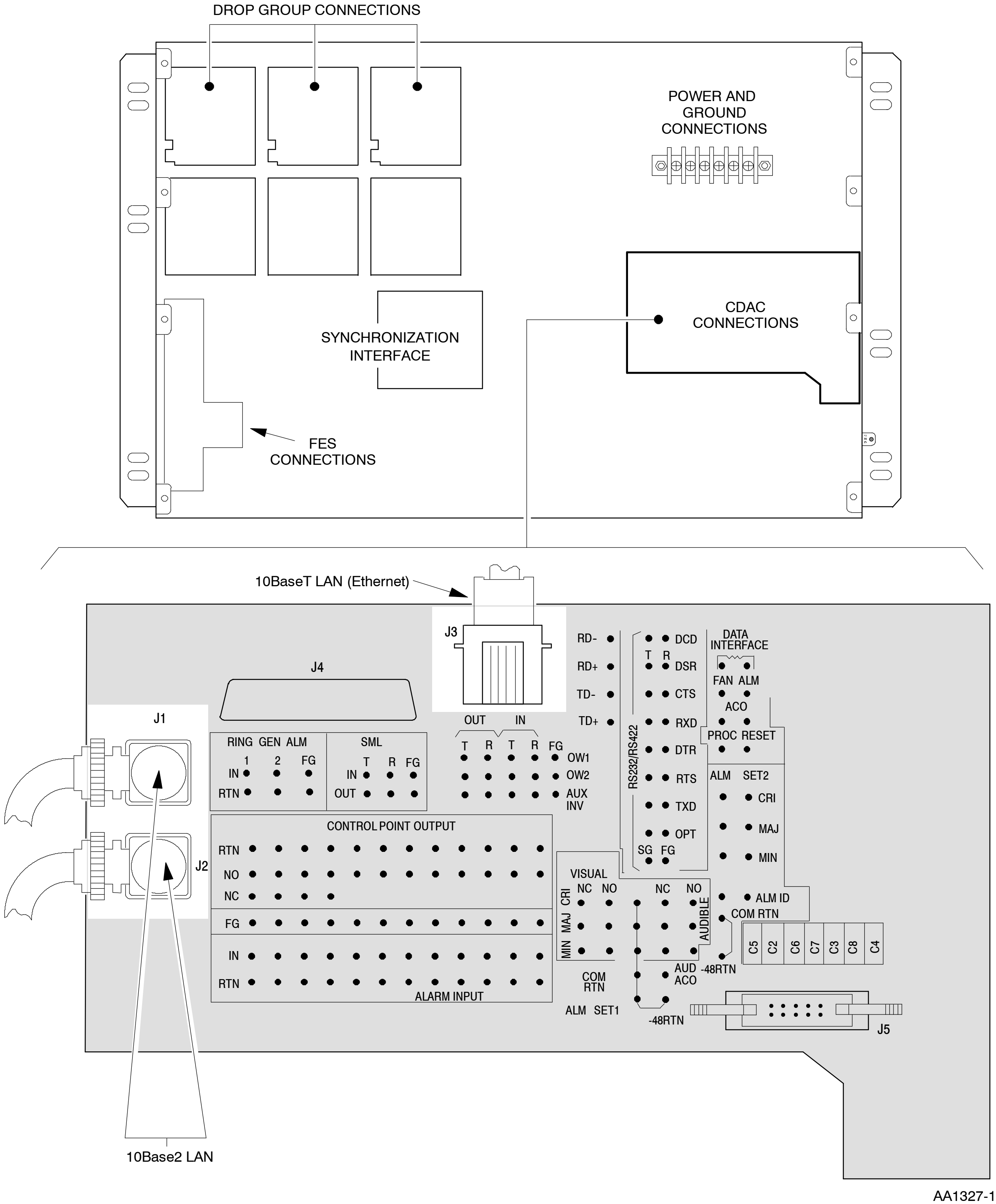


Figure 1. 1603 SMX Rear View

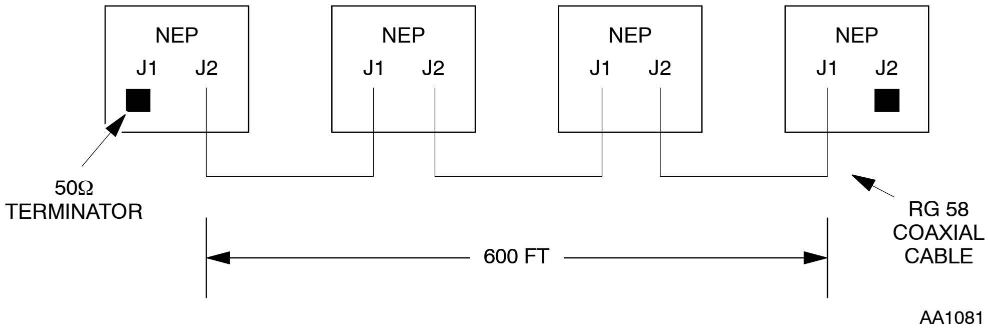
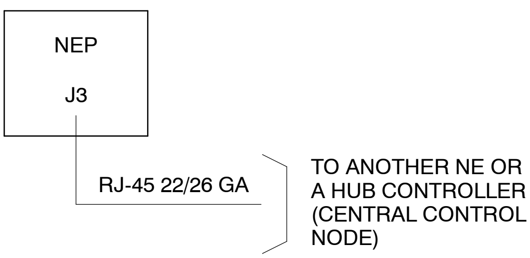


Figure 2. 10Base2 LAN Interface



CONTACT	SIGNAL
1	TD+
2	TD-
3	RD+
4	N/C
5	N/C
6	RD-
7	N/C
8	N/C

N/C = NO CONNECTION

AA1082

Figure 3. 10BaseT LAN Interface

9 Connect RJ-45 plug to connector J3 (NEP) on the 1603 SMX shelf.

10 Connect other end of cable to appropriate port on central control node equipment.

11 STOP. This procedure is complete.

DLP-022
Test DS1/DS3 Facilities Using MTA101 Plug-in Unit

Purpose

This procedure describes provisions related to testing DS1/DS3 facilities using the Metallic Test Access 101 (MTA101) plug-in unit.

STEP	PROCEDURE
1	**CAUTION: Possibility of service interruption. Use of the MTA101 unit results in traffic loss for any VTG or LDR slots that are carrying traffic.**
2	***WARNING: Possibility of damage to equipment. This equipment contains static-sensitive devices. Refer to DLP-002 for special handling instructions.***
3	**NOTE:** *The MTA101, 625643-000-001 (see Figure 1), is a passive plug-in unit that provides front access to metallic lines connected to the 1603 SMX shelf. By inserting the MTA101 into one of the VTG or LDR slots on the 1603 SMX shelf, the DS1 or DS3 circuits wired to that slot can be accessed using the MTA101 front panel mounted test connectors. Figure 2 shows this arrangement.* **NOTE:** *For DS1, the MTA101 provides dual Bantam style jacks (one for input and one for output connections) - one pair of jacks for each of the four DS1 circuits on the VTG plug-in units. The DS1 test jacks provide direct coupling to the facility pairs for dc continuity testing.* **NOTE:** *For DS3, the MTA101 provides two WECO440 style coaxial connectors (one for input and one for output). The test jacks are AC-coupled to the facility and dc testing is not possible.* **NOTE:** *The MTA101 does not work with LDR501.* Is slot wired for DS1 (VTG) or DS3 (LDR) being tested? If DS1, go to step 11. If DS3, go to step 4.

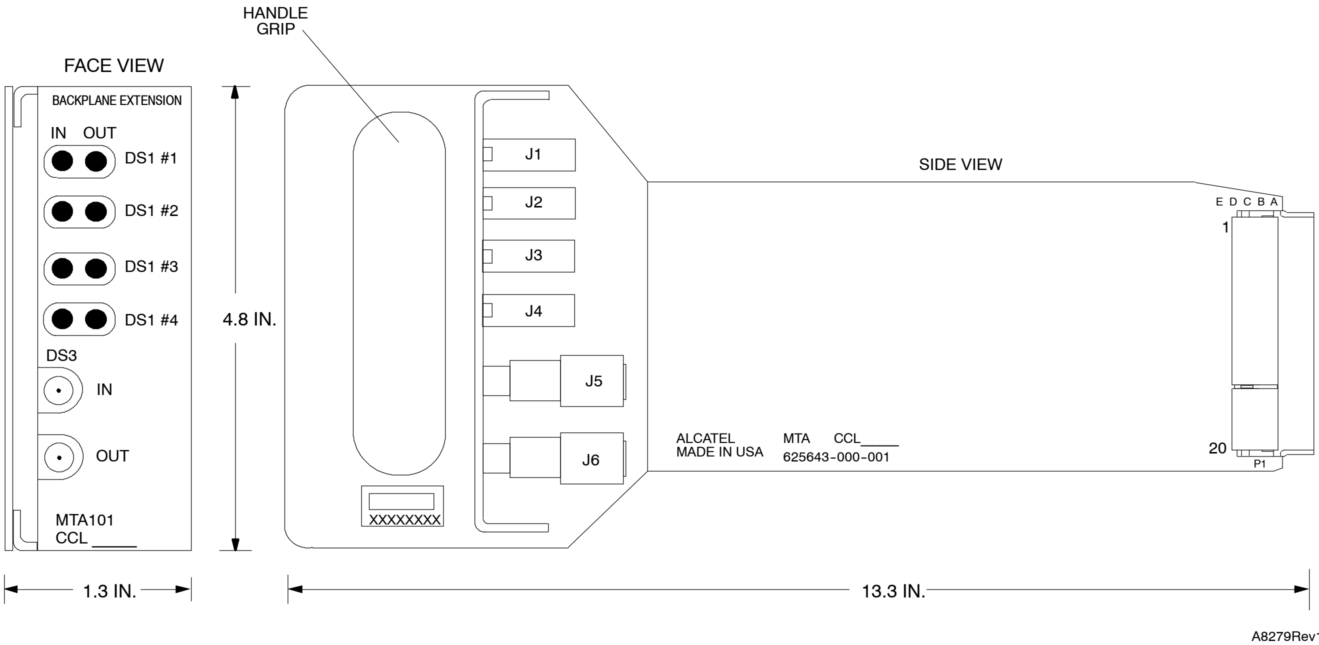


Figure 1. MTA101 Plug-in Unit

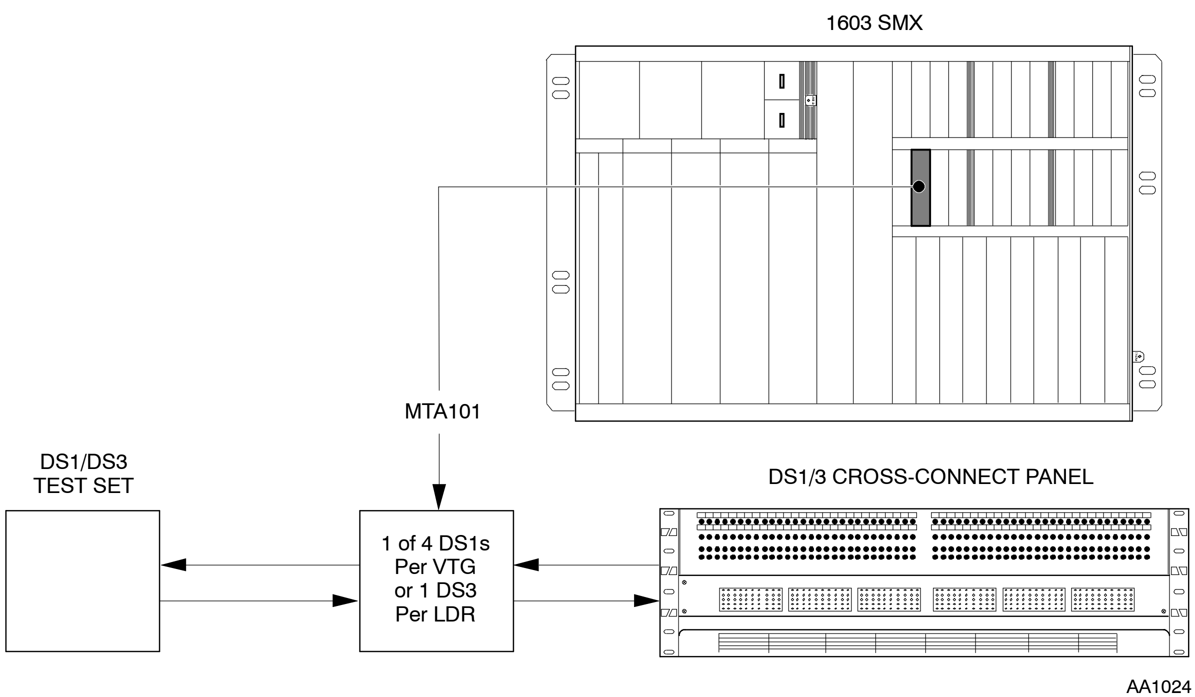


Figure 2. MTA101 Application

DS3 Test Connections

4 ***NOTE:*** *Changing the Service State is optional; it prevents alarms from occurring when plug-in units are removed.*

NOTE: *The MTA101 does not work with LDR501.*

If LDR units for DS3 port being tested are installed and in-service, change service state to maintenance:

a. In the scope pane, expand Equipment and select LDR.

b. In the result pane, right-click LDRs being placed in maintenance to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select Maintenance.

e. On the toolbar, select Submit; then close work view.

5 If installed, remove both LDR units (LDR-xA and LDR-xB) for DS3 port being tested.

6 Insert the MTA101 into either LDR slot xA or xB. Both slots are wired to the same facility connections on the backplane.

7 Connect test equipment to DS3 IN and OUT test jacks on MTA101 unit (see Figure 1).

8 When testing is complete, remove MTA101 and reinstall LDR units (if previously installed).

9 If LDRs were placed in maintenance state (step 4), change service state:

a. In the scope pane, expand Equipment and select LDR.

b. In the result pane, right-click LDRs being placed in service to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select In Service.

e. On the toolbar, select Submit; then close work view.

10 STOP. This procedure is complete.

DS1 Test Connections

11 Is VTG unit equipped and assigned (entered into service)?

If yes, go to step 12.
If no, go to step 16.

12 For VTG (Drop Group and Port number) being removed, inhibit switching to protection:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click VTG being removed to display a context menu.

c. From context menu, select **Task>Provision>Allow/Inhibit** to display a work view.

d. From the Sw to Prot drop-down list, select Inhibit.

e. On the toolbar, select Submit; then close work view.

13 Is VTG unit active?

If yes, go to step 15
If no, go to step 14.

14 Switch VTG unit to active:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click VTG being tested to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to display a work view.

d. Select VTG being tested.

e. In the Switch Mode region, select Manual radio button.

f. On the toolbar, select Submit; then close work view.

15 ***NOTE:*** *Changing the Service State is optional; it prevents alarms from occurring when plug-in units are removed.*

Change service state of VTG to maintenance:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click VTG being placed in maintenance to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select Maintenance.

e. On the toolbar, select Submit; then close work view.

16 If necessary, remove the VTG unit in slot being tested.

17 Insert the MTA101 into the VTG slot.

18 Connect test equipment to Bantam test jacks for DS1 facility being tested.

19 When testing is complete, remove MTA101 and reinstall VTG (if previously installed).

20 If switching was inhibited (step 12), perform the following to allow switching:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click VTG being removed to display a context menu.

c. From the context menu, select **Task>Provision>Allow/Inhibit** to display a work view.

d. From the Sw to Prot drop-down list, select Inhibit.

e. On the toolbar, select Submit; then close work view.

21 If VTG was placed in maintenance state (step 15), place unit back in service:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click VTG being placed in service to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select In Service.

e. On the toolbar, select Submit; then close work view.

22 STOP. This procedure is complete.

DLP-023
Test DS1 Loopbacks

Purpose

This procedure describes how to test DS1 loopbacks.

STEP	PROCEDURE

1 **CAUTION: Possibility of service interruption. Performing loopbacks interrupts traffic.**

2 Place port in maintenance state:

a. In the scope pane, expand Facility and select DS1.

b. In the result pane, right-click DS1 port being tested to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select Maintenance.

e. On the toolbar, select Submit; then close work view.

3 See Figure 1. If a test signal is available from the far-end NE, operate a loopback toward the network (terminal):

a. In the scope pane, expand Equipment and select DS1.

b. In the result pane, right-click DS1 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Terminal.

e. On the toolbar, select Submit; then close work view.

NOTE: *Terminal loopback is not valid for LIF601 (DS3/DS1 transmux).*

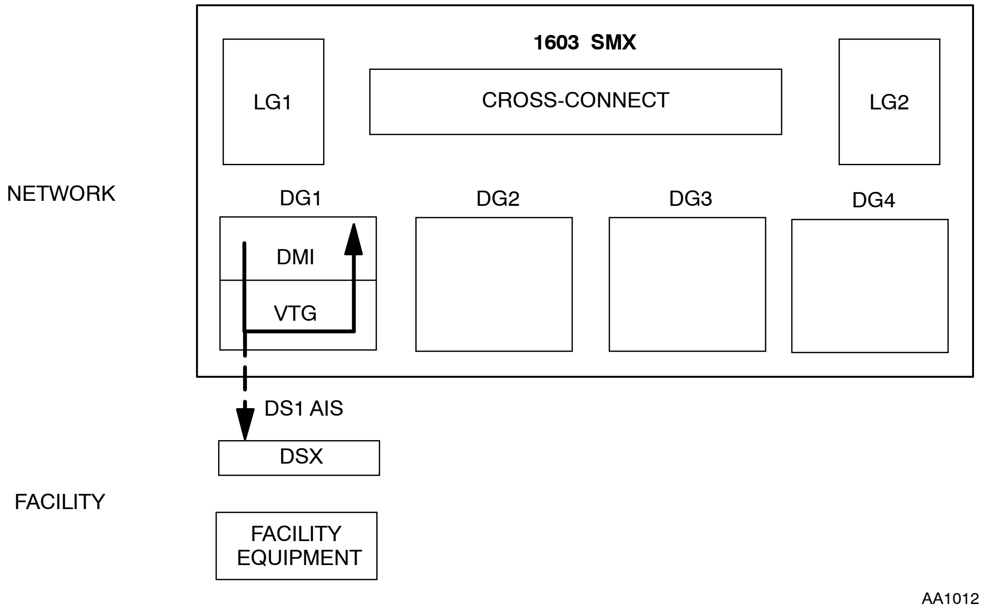


Figure 1. DS1 Loopback toward Terminal (NE)

4 Verify the test signal is looped back to the NE at the sending end.

5 Release the loopback:

a. In the scope pane, expand Equipment and select DS1.

b. In the result pane, right-click DS1 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

6 See Figure 2. If a test signal is available from the facility, operate a loopback toward the facility:

a. In the scope pane, expand Equipment and select DS1.

b. In the result pane, right-click DS1 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Facility:N,F.

e. On the toolbar, select Submit; then close work view.

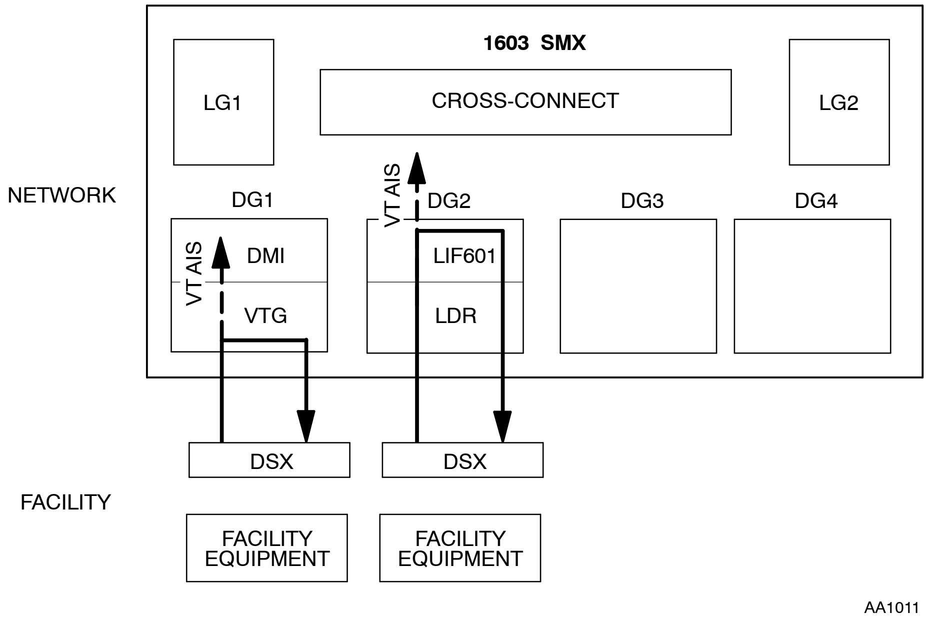


Figure 2. DS1 Loopback toward Facility

7 Verify the test signal is looped back to the facility equipment.

8 Release the loopback:

a. In the scope pane, expand Equipment and select DS1.

b. In the result pane, right-click DS1 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

9 See Figure 3. If far-end facility equipment can accept loop-up code, perform the following:

a. In the scope pane, expand Equipment and select DS1.

b. In the result pane, right-click DS1 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Facility:N,F.

e. On the toolbar, select Submit; then close work view.

NOTE: *If facility equipment is another 1603 SMX NE, it must be provisioned to allow automatic loopbacks per step 12.*

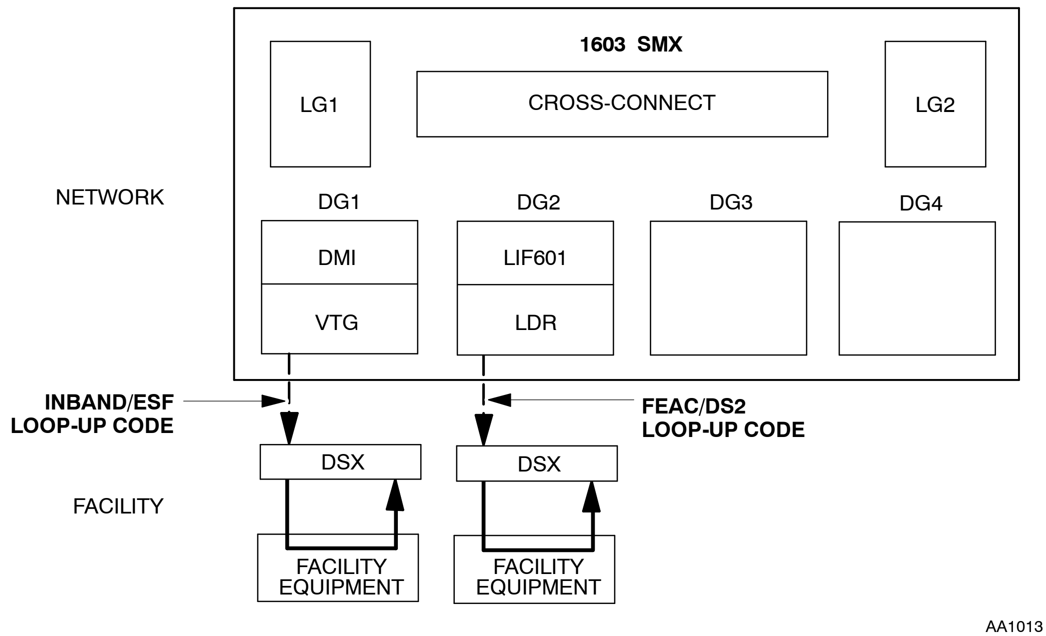


Figure 3. Sending Inband CSU Loop-Up Code to Facility Equipment

10 Verify the facility equipment is looped back toward the NE.

11 Release the loopback:

a. In the scope pane, expand Equipment and select DS1.

b. In the result pane, right-click DS1 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

12 See Figure 4. To allow external loopback request on DS1 port, perform the following:

a. In the scope pane, expand Equipment and select DS1.

b. In the result pane, right-click DS1 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Facility:N,F.

e. On the toolbar, select Submit; then close work view.

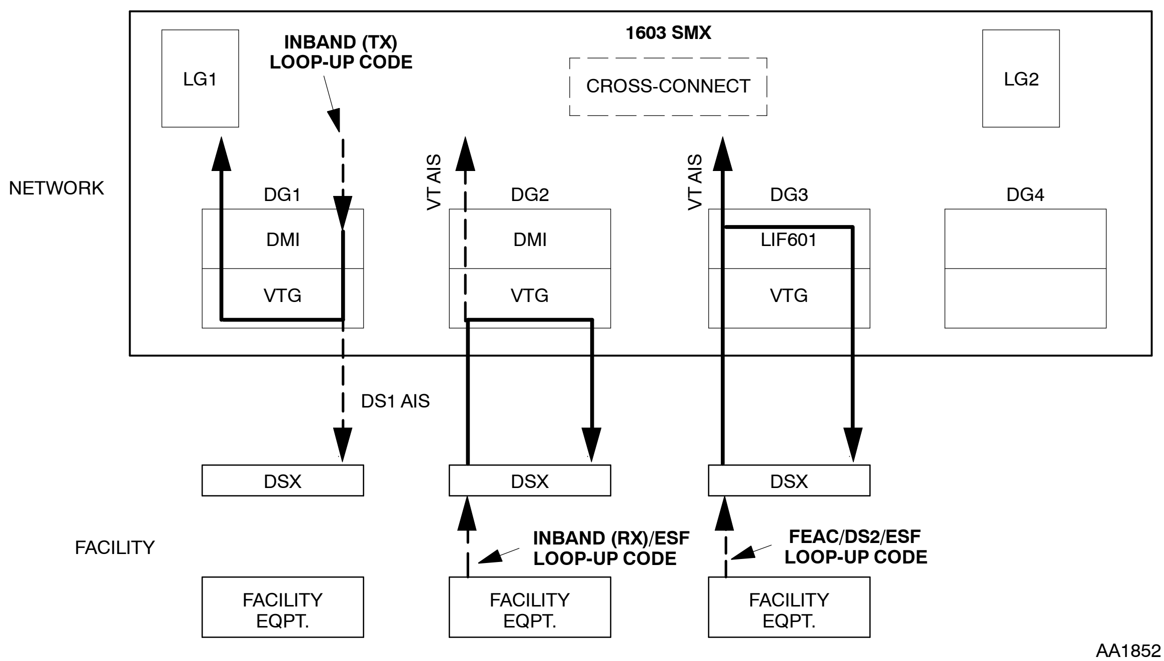


Figure 4. Receiving Inband Loopback Code from Facility Equipment

13 Send loopback code from facility equipment. At facility equipment, verify test signal is looped back.

14 Send code to release loopback. Verify loopback is released.

15 If required by company policy, inhibit automatic loopback:

NOTE: *External loopback capability should not be left enabled.*

a. In the scope pane, expand Equipment and select DS1.

b. In the result pane, right-click DS1 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Facility:N,F.

e. On the toolbar, select Submit; then close work view.

16 When loopback tests are completed, place port in required service state:

a. In the scope pane, expand Facility and select DS1.

b. In the result pane, right-click DS1 port being returned to original service state to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select In-Service or Memory Administration (as required).

e. On the toolbar, select Submit; then close work view.

17 STOP. This procedure is complete.

DLP-024
Test DS3 Loopbacks

Purpose

This procedure describes how to test DS3 loopbacks.

STEP	PROCEDURE

1 **CAUTION: Possibility of service interruption. Performing loopbacks interrupts traffic.**

2 Place port in maintenance state:

a. In the scope pane, expand Facility and select DS3.

b. In the result pane, right-click DS3 port being tested to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select Maintenance.

e. On the toolbar, select Submit; then close work view.

3 See Figure 1. If a test signal is available from the far-end NE, operate a loopback toward the network (terminal):

a. In the scope pane, expand Facility and select DS3.

b. In the result pane, right-click DS3 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Terminal.

e. On the toolbar, select Submit; then close work view.

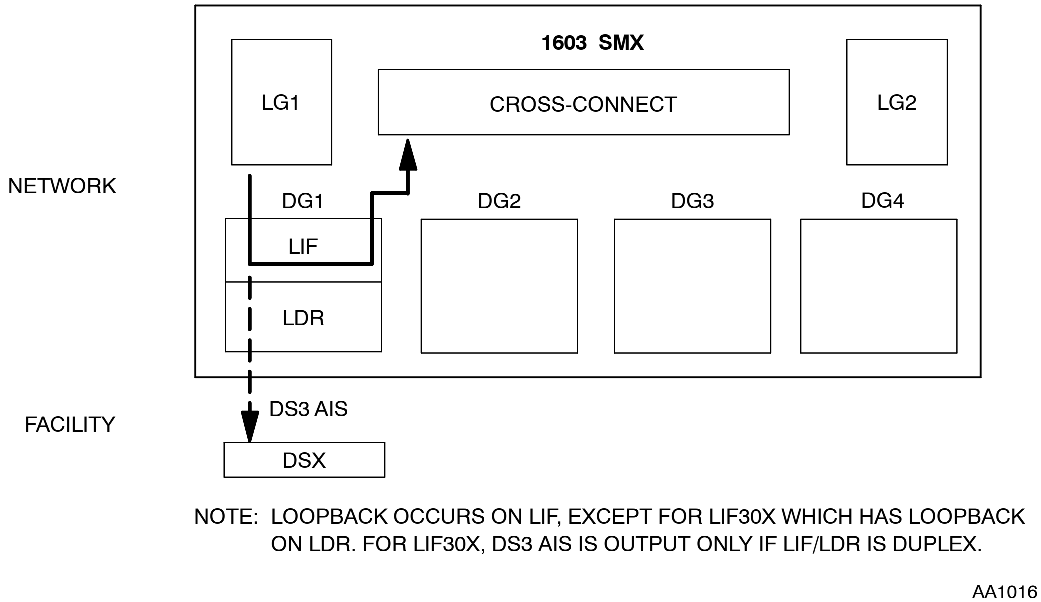


Figure 1. DS3 Loopback Toward Terminal (NE)

4 Verify the test signal is looped back to the NE at the sending end.

5 Release the loopback:

a. In the scope pane, expand Facility and select DS3.

b. In the result pane, right-click DS3 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

6 See Figure 2. If a test signal is available from the facility, operate a loopback toward the facility:

a. In the scope pane, expand Facility and select DS3.

b. In the result pane, right-click DS3 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Facility:N,F.

e. On the toolbar, select Submit; then close work view.

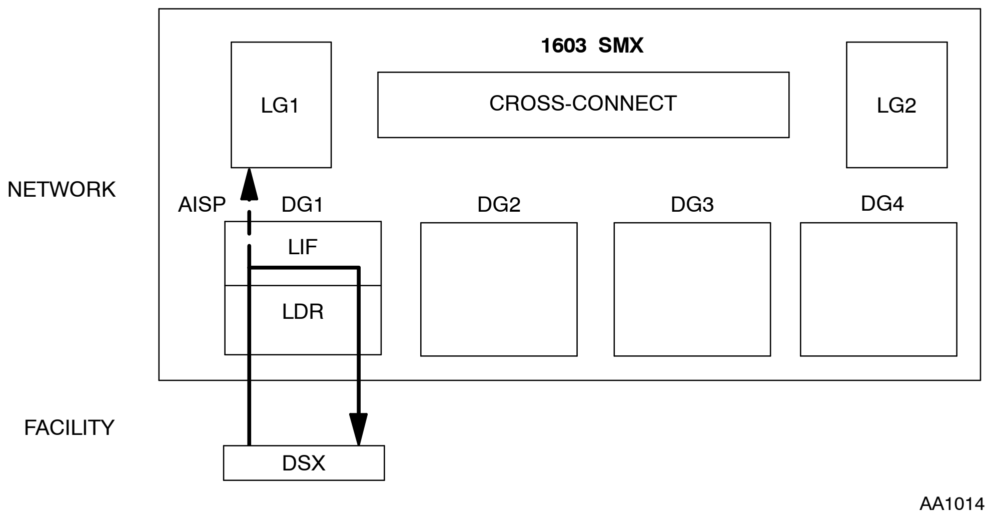


Figure 2. DS3 Loopback Toward Facility

7 Verify the test signal is looped back to the facility equipment.

8 Release the loopback:

a. In the scope pane, expand Facility and select DS3.

b. In the result pane, right-click DS3 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

9 See Figure 3. If far-end facility equipment can accept loop-up code, perform the following (requires LIF601):

a. In the scope pane, expand Facility and select DS3.

b. In the result pane, right-click DS3 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Facility:N,F.

e. On the toolbar, select Submit; then close work view.

NOTE: *If far-end facility equipment is a 1603 SMX, a 1603 SM, or a 1603 SE, it must be provisioned to allow automatic loopbacks per step 12.*

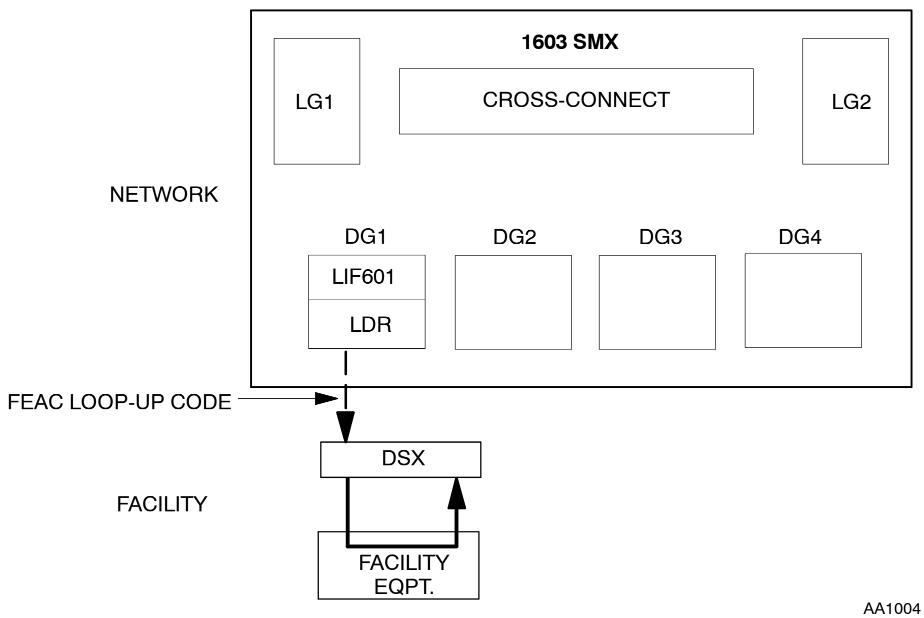


Figure 3. Sending FEAC Loop-up Code to Facility Equipment

10 Verify the facility is looped back toward the NE.

11 Release the loopback:

a. In the scope pane, expand Facility and select DS3.

b. In the result pane, right-click DS3 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

12 See Figure 4. Allow external loopback request on DS3 port (requires LIF601):

a. In the scope pane, expand Equipment and select DS3.

b. In the result pane, right-click DS3 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Facility:N,F.

e. On the toolbar, select Submit; then close work view.

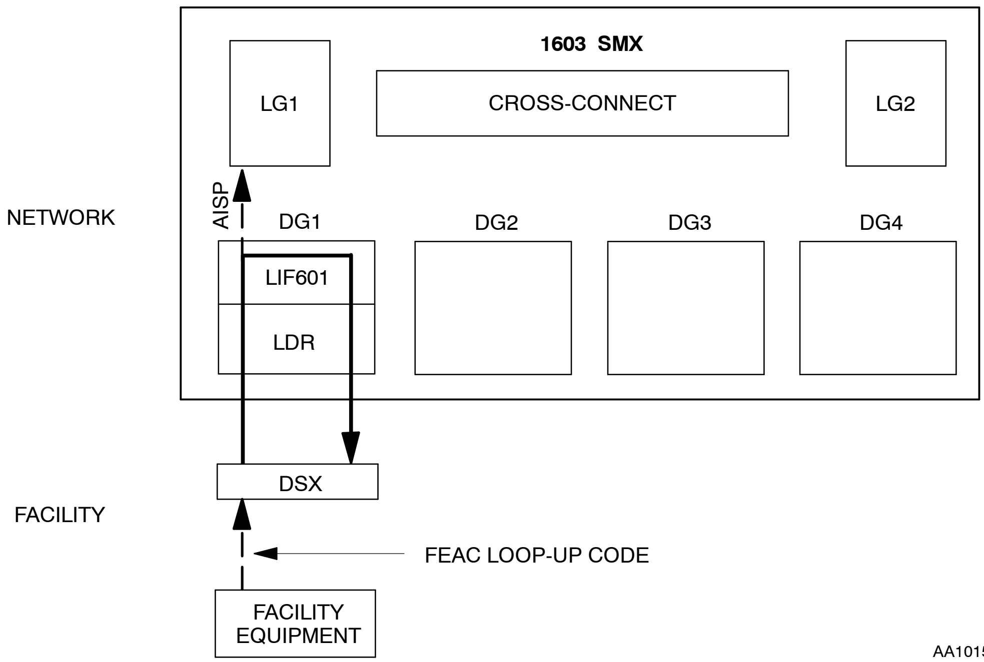


Figure 4. Receiving FEAC Loop-up Code from Facility Equipment

13 Send loopback code from facility equipment. At facility equipment, verify test signal is looped back.

14 Send code to release loopback. Verify loopback is released.

15 If required by company policy, inhibit remote loopback:

NOTE: *External loopback capability should not be left enabled.*

a. In the scope pane, expand Equipment and select DS3.

b. In the result pane, right-click DS3 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Facility:N,F.

e. On the toolbar, select Submit; then close work view.

16 When loopback tests are completed, place port in required service state:

a. In the scope pane, expand Facility and select DS3.

b. In the result pane, right-click DS3 port being returned to original service state to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select In-Service or Memory Administration (as required).

e. On the toolbar, select Submit; then close work view.

17 STOP. This procedure is complete.

DLP-025
Test EC1 Loopbacks

Purpose

This procedure describes how to test EC1 loopbacks.

STEP	PROCEDURE

1 **CAUTION: Possibility of service interruption. Performing loopbacks interrupts traffic.**

2 ***NOTE:*** *Loopbacks (facility or terminal) are not allowed while input synchronization messaging is enabled for the same facility. If necessary, edit the facility to disable input synchronization messaging.*

Place port in maintenance state:

a. In the scope pane, expand Facility and select EC1.

b. In the result pane, right-click EC1 being tested to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select Maintenance.

e. On the toolbar, select Submit; then close work view.

3 See Figure 1. If a test signal is available from the far-end NE, operate a loopback toward the network (terminal):

a. In the scope pane, expand Equipment and select EC1.

b. In the result pane, right-click EC1 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Terminal.

e. On the toolbar,select Submit; then close work view.

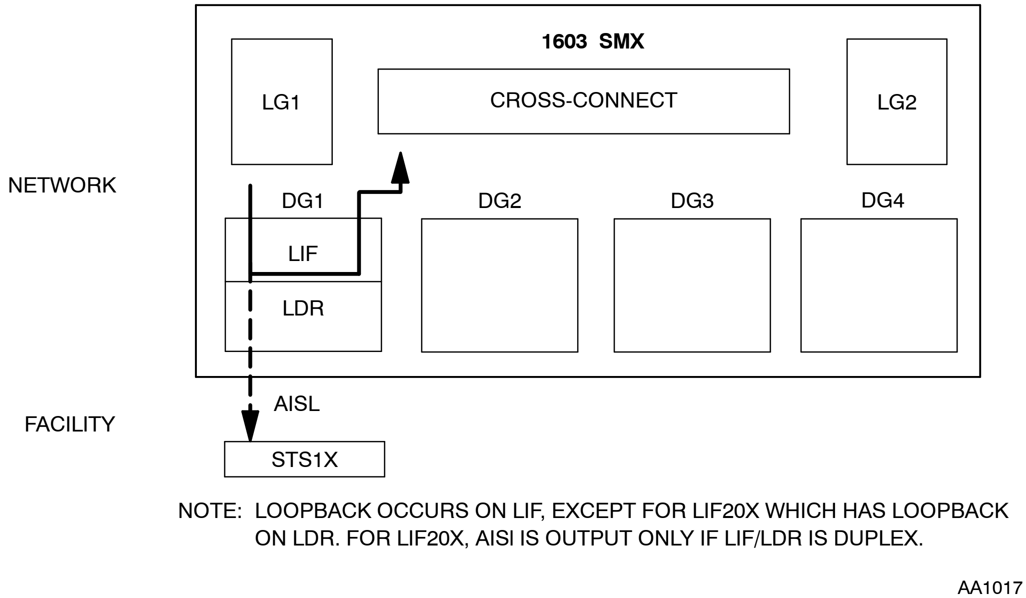


Figure 1. EC1 Loopback Toward Terminal (NE)

4 Verify the test signal is looped back to the NE at the sending end.

5 Release the loopback:

a. In the scope pane, expand Equipment and select EC1.

b. In the result pane, right-click EC1 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

6 See Figure 2. If a test signal is available from the facility, operate a loopback toward the facility:

a. In the scope pane, expand Equipment and select EC1.

b. In the result pane, right-click EC1 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Facility:N,F.

e. On the toolbar, select Submit; then close work view.

NOTE: *This task is performed using TL1 commands.*

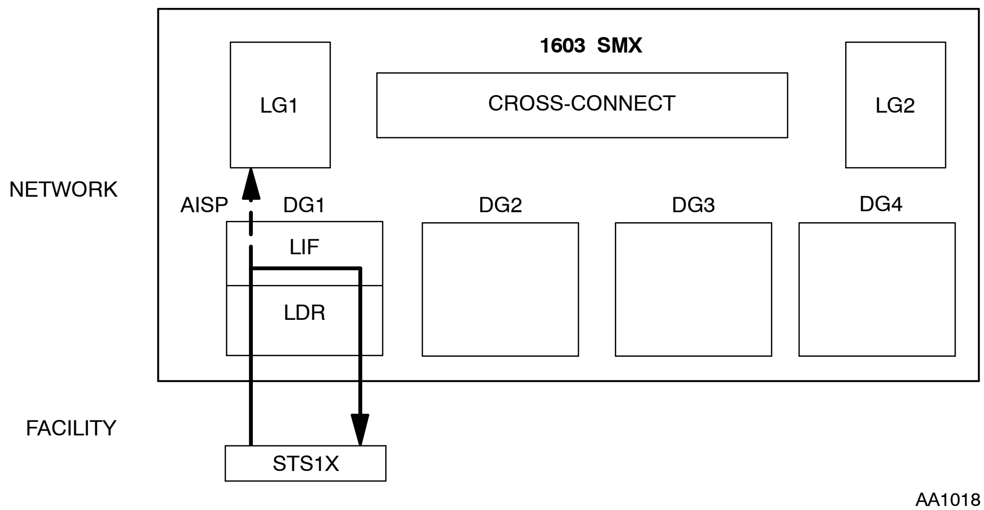


Figure 2. EC1 Loopback Toward Facility

7 Verify the test signal is looped back to the facility equipment.

8 Release the loopback:

a. In the scope pane, expand Equipment and select EC1.

b. In the result pane, right-click EC1 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

9 When loopback tests are completed, place port in required service state:

a. In the scope pane, expand Facility and select EC1.

b. In the result pane, right-click EC1 being returned to original service state to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select In Service or Memory Administration (as required).

e. On the toolbar, select Submit; then close work view.

10 STOP. This procedure is complete.

DLP-026
Test OC3 Loopbacks

Purpose

This procedure describes how to test OC3 loopbacks.

STEP	PROCEDURE
1	**CAUTION: Possibility of service interruption. Placing the OC3 facility in maintenance state causes a line AIS (alarm insertion signal) to be transmitted on the OC3 facility. If the facility is active, it causes a line switch (linear configuration) or (STS3c, STS1 and/or VT1) path switch (ring configuration). This may interrupt service if a protection line or protecting path is not available.**
2	***NOTE:*** *Loopbacks (facility or terminal) are not allowed while input synchronization messaging is enabled for the same facility. If necessary, edit the facility to disable input synchronization messaging.* Place facility being looped in maintenance state: a. In the scope pane, expand Facility and select OC3. b. In the result pane, right-click OC3 being tested to display a context menu. c. From the context menu, select **Provision Parameters** to display a work view. d. From the Service State drop-down list, select Maintenance. e. On the toolbar, select Submit; then close work view.

3 See Figure 1. Operate a loopback toward the NE (terminal):

a. In the scope pane, expand Equipment and select OC3.

b. In the result pane, right-click OC3 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Terminal.

e. On the toolbar, select Submit; then close work view.

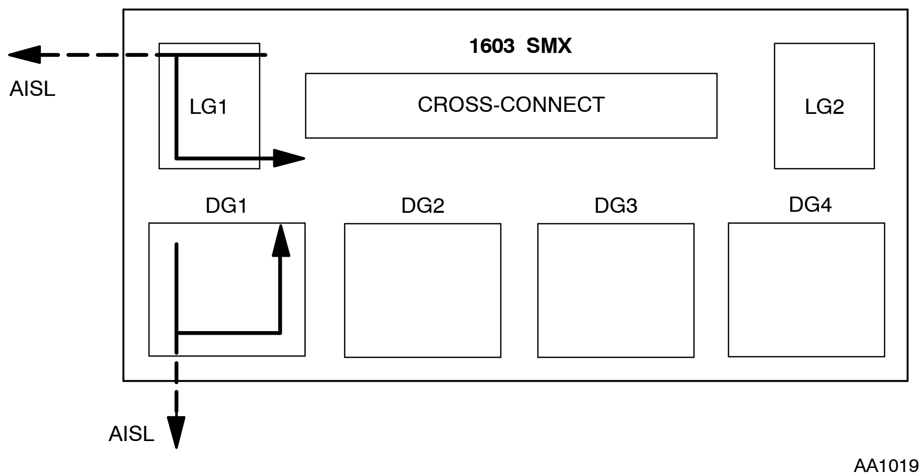


Figure 1. OC3 Loopback Toward Terminal (NE)

4 Verify the test signal is looped back to the sending end.

5 Release the loopback:

a. In the scope pane, expand Equipment and select OC3.

b. In the result pane, right-click OC3 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

6 See Figure 2. Operate a loopback toward the facility:

a. In the scope pane, expand Equipment and select OC3.

b. In the result pane, right-click OC3 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Facility:N,F.

e. On the toolbar, select Submit; then close work view.

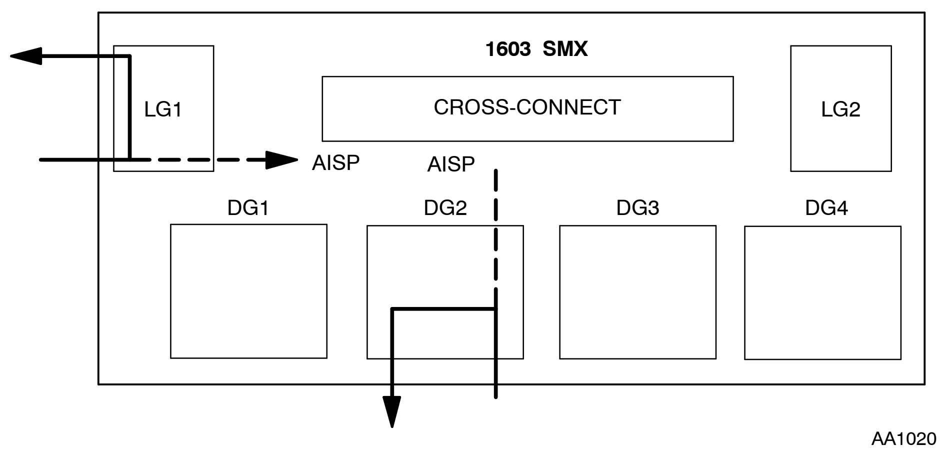


Figure 2. OC3 Loopback Toward Facility

7 Verify the test signal is looped back to the sending end.

8 Release the loopback:

a. In the scope pane, expand Equipment and select OC3.

b. In the result pane, right-click OC3 being removed to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

9 When loopback tests are completed, place OC3 in required service state:

a. In the scope pane, expand Facility and select OC3.

b. In the result pane, right-click OC3 being returned to original service state to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select In Service or Memory Administration (as required).

e. On the toolbar, select Submit; then close work view.

10 STOP. This procedure is complete.

DLP-027
Test OC12 Loopbacks

Purpose

This procedure describes how to test OC12 loopbacks.

STEP	PROCEDURE
1	**CAUTION: Possibility of service interruption. Placing the OC12 facility in maintenance state causes a line AIS (alarm insertion signal) to be transmitted on the OC12 facility. If the facility is active, it causes a line switch (linear configuration) or (STS12c, STS3c, STS1 and/or VT1) path switch (ring configuration). This may interrupt service if a protection line or protecting path is not available.**
2	***NOTE:*** *Loopbacks (facility or terminal) are not allowed while input synchronization messaging is enabled for the same facility. If necessary, disable input synchronization messaging.* Place facility being tested in maintenance state: a. In the scope pane, expand Facility and select OC12. b. In the result pane, right-click OC12 being tested to display a context menu. c. From the context menu, select **Provision Parameters** to display a work view. d. From the Service State drop-down list, select Maintenance. e. On the toolbar, select Submit; then close work view.

3 See Figure 1. Operate a loopback toward the NE (terminal):

a. In the scope pane, expand Facility and select OC12.

b. In the result pane, right-click OC12 being tested to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Terminal.

e. On the toolbar, select Submit; then close work view.

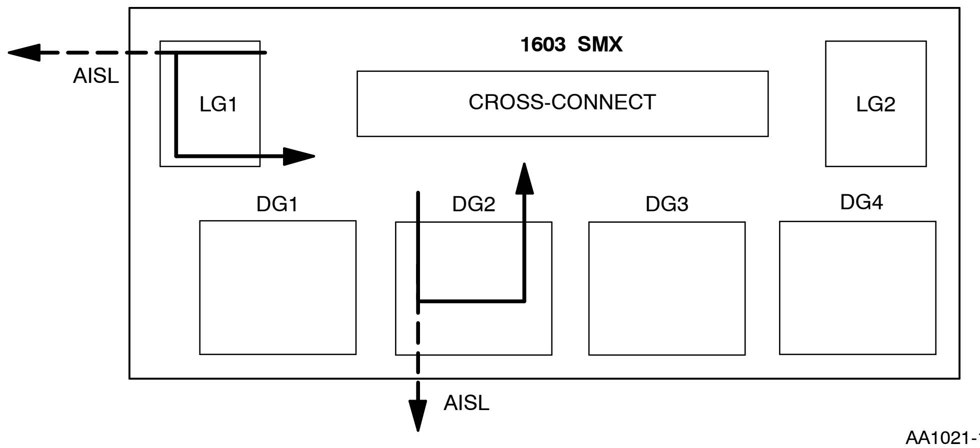


Figure 1. OC12 Loopback Toward Terminal (NE)

4 Verify the test signal is looped back to the sending end.

5 Release the loopback:

a. In the scope pane, expand Facility and select OC12.

b. In the result pane, right-click OC12 being tested to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

6 See Figure 2. Operate a loopback toward the facility:

a. In the scope pane, expand Facility and select OC12.

b. In the result pane, right-click OC12 being tested to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Facility:N,F.

e. On the toolbar, select Submit; then close work view.

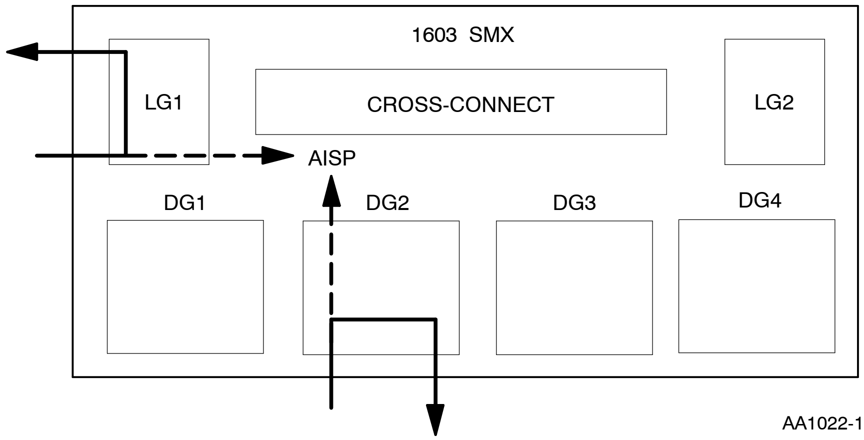


Figure 2. OC12 Loopback Toward Facility

7 Verify the test signal is looped back to the sending end.

8 Release the loopback:

a. In the scope pane, expand Facility and select OC12.

b. In the result pane, right-click OC12 being tested to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

9 When loopback tests are completed, place OC12 in required service state:

a. In the scope pane, expand Facility and select OC12.

b. In the result pane, right-click OC12 being returned to original service state to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select In Service or Memory Administration (as required).

e. On the toolbar, select Submit; then close work view.

10 STOP. This procedure is complete.

DLP-028
Test DS1/VT1 Using Test Access Feature

Purpose

This procedure describes how to use the Test Access feature to test a DS1 or a VT1. This feature only works on dropped VTs and DS1; it will not work on through VTs.

Prerequisite

This procedure assumes the DS1 or VT1 to be tested is assigned and cross-connected.

STEP	PROCEDURE

1 **CAUTION: Possibility of service interruption. This procedure is service-affecting if SPLIT or LOOP access modes are used.**

2 Perform the following steps to verify and assign (if necessary) the DS1 port to be used as the Test Access Port (TACCT1):

a. In the scope pane, expand Facility and select DS1.

b. In the result pane, right-click DS1 port being used as the test access port to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select Memory Administration.

e. Use the Equalization Distance spin-box to select the correct equalization distance. (The distance for 22 gauge wire ranges from 0 to 655 feet. Default = 0.)

f. On the toolbar, select Submit; then close work view.

3 Select DS1 port to be used as the TACCT1:

NOTE: *This task is performed using TL1 commands.*

a. In the scope pane, right-click on NE name to display a context menu.

b. From the context menu, select **Task>TL1 Direct Entry** to display a TL1 Direct Entry work view.

c. From the TL1 Command drop-down list, select the **SET-NE-ALL:...** template.

d. Modify the template to create the following command line with the appropriate parameter values: **SET-NE-ALL::COM::::TACCT1=aidt1;**

where: aidt1 = DGy-T1-vtgrp-vtno (format for grouped numbering of ports)
y =1, 2, 3, or 4
vtgrp = 1...7
vtno = 1...4
= DGy-T1-pathno (format for sequential numbering of ports)

y = 1, 2, 3, or 4
pathno = 1...28 (DS1 port number)

e. Select Send.

4 Is a DS1 or a VT1 being tested?

If DS1, go to step 5.
If VT1, go to step 10.

5 If SPLIT or LOOP test modes will be used, place DS1 to be tested in maintenance state:

a. In the scope pane, expand Facility and select DS1.

b. In the result pane, right-click DS1 being tested to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select Maintenance.

e. On the toolbar, select Submit; then close work view.

6 Connect T1 being tested to the TACCT1:

NOTE: *If an active test session is already in place, you can select another DS1 to test; however, only one session is active at a time.*

NOTE: *This task is performed using TL1 commands.*

a. In the scope pane, right-click on NE name to display a context menu.

b. From the context menu, select **Task>TL1 Direct Entry** to display a TL1 Direct Entry work view.

c. From the TL1 Command drop-down list, select the **CONN-TACC-T1:...** template.

d. Modify the template to create the following command line with the appropriate parameter values: **CONN-TACC-T1::aidt1:::tap:mode;**

where:	aidt1 =	DGy-T1-pathno (format for sequential numbering of ports) y = 1, 2, 3, or 4 pathno = 1...28 (DS1 port number)
	=	DGy-T1-vtgrp-vtno (format for grouped numbering of ports) y = 1, 2, 3, or 4 vtgrp = 1...7 (VT1.5 group number) vtno = 1...4 (VT1.5 path number)
	tap =	1...999 (test access session number; select any number. Default 1.
	mode =	MONE, MONF, SPLTA, SPLTB, SPLTF, LOOPE, or LOOPF

e. Select Send.

NOTE: *See Figure 1 for 2WAY connections, Figure 2 for 2WAYPR connections, and Figure 3 for 2WAYBR connections.*

NOTE: *To disconnect the test session, select Delete.*

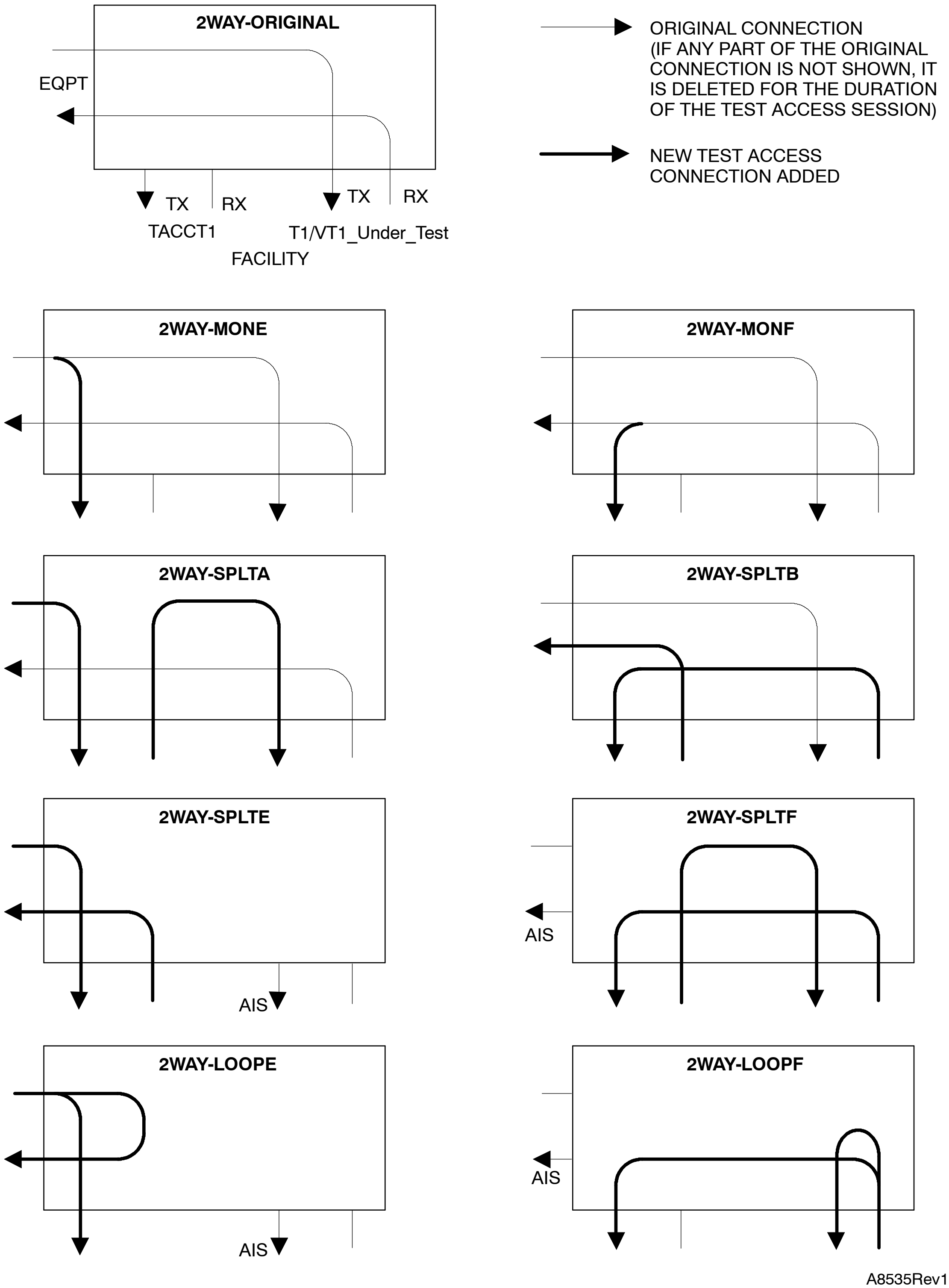


Figure 1. Test Access Connections for 2WAY Cross-Connection

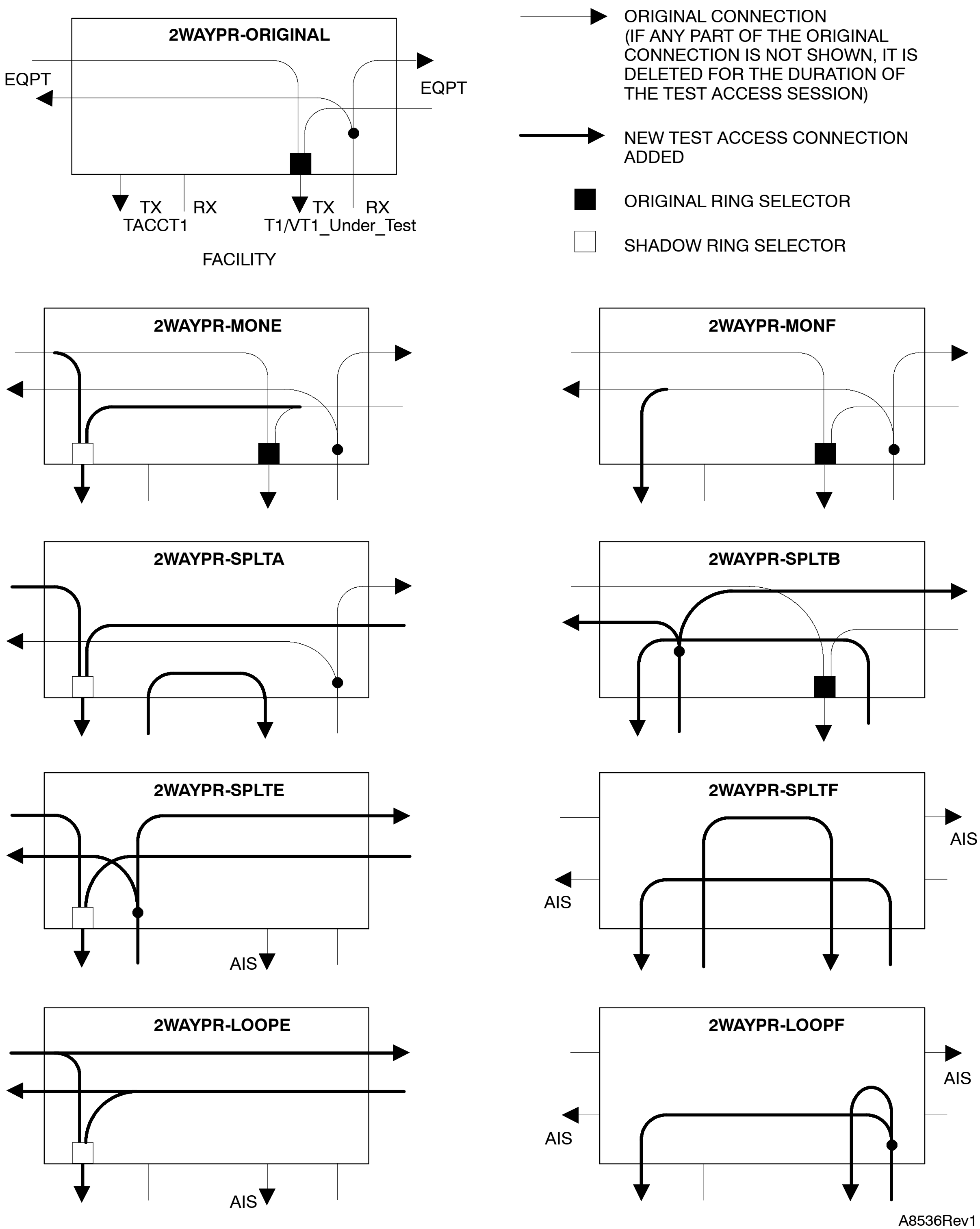


Figure 2. Test Access Connections for 2WAYPR Cross-Connection

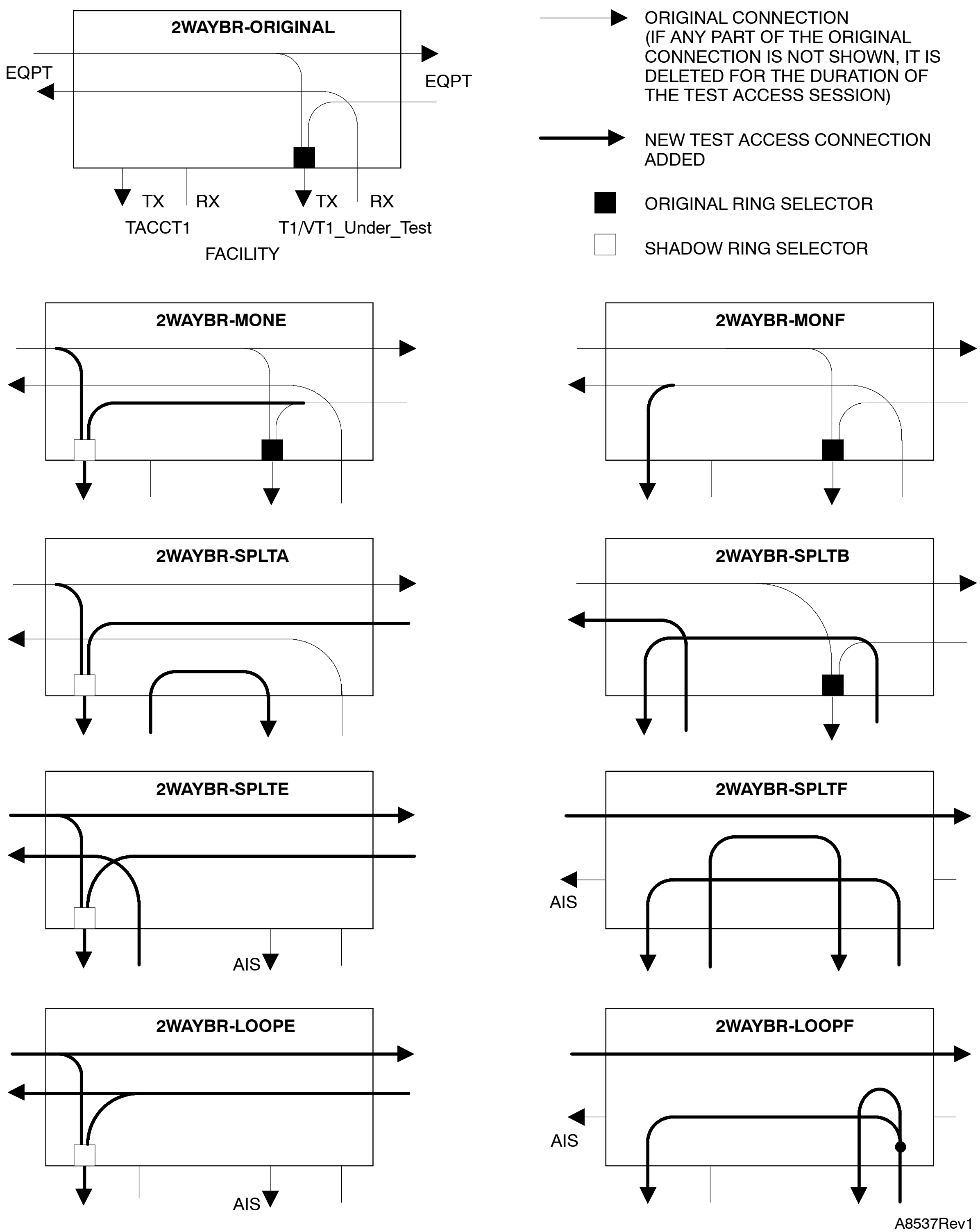


Figure 3. Test Access Connections for 2WAYBR Cross-Connection

7 If T1 Under Test is in maintenance state, and you want to return it to In-Service (IS) or memory administration (OOS-MA) state, perform the following:

a. In the scope pane, expand Facility and select DS1.

b. In the result pane, right-click DS1 being returned to original service state to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select In Service or Memory Administration (as required).

e. On the toolbar, select Submit; then close work view.

8 Repeat from step 5 for next DS1 to be tested.

9 STOP. This procedure is complete.

10 Place VT1 to be tested in memory administration (OOS-MA) if SPLIT or LOOP test modes will be used:

a. In the scope pane, expand Facility; then expand DS1 and select VT1.

b. In the result pane, right-click VT1 being tested to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select Memory Administration.

e. On the toolbar, select Submit; then close work view.

11 Connect VT1 being tested to the TACCT1:

NOTE: *If an active test session is already in place, you can select another DS1 to test; however, only one session is active at a time.*

NOTE: *This task is performed using TL1 commands.*

a. In the scope pane, right-click on NE name to display a context menu.

b. From the context menu, select **Task>TL1 Direct Entry** to display a TL1 Direct Entry work view.

c. From the TL1 Command drop-down list, select the **CONN-TACC-T1:...** template.

d. Modify the template to create the following command line with the appropriate parameter values: **CONN-TACC-T1::aidt1:::tap:mode;**

where:

aidt1 = DGy-VT1-pathno (format for sequential numbering of ports)

y = 1, 2, 3, or 4
pathno = 1...28 (DS1 port number)

= DGy-VT1-vtgrp-vtno (format for grouped numbering of ports)

y = 1, 2, 3, or 4
vtgrp = 1...7 (VT1.5 group number)
vtno = 1...4 (VT1.5 path number)

tap = 1...999 (test access session number; select any number. Default 1.

mode = MONE, MONF, SPLTA, SPLTB, SPLTF, LOOPE, or LOOPF

e. Select Send.

NOTE: *See Figure 1 for 2WAY connections, Figure 2 for 2WAYPR connections, and Figure 3 for 2WAYBR connections.*

NOTE: *To disconnect the test session, select Delete.*

12 If VT1 under test is in memory administration state, and you want to return it to In Service (IS), perform the following steps:

a. In the scope pane, expand Facility; then expand DS1 and select VT1.

b. In the result pane, right-click VT1 being returned to service to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select In Service.

e. On the toolbar, select Submit; then close work view.

13 Repeat from step 10 for next VT1 to be tested.

14 STOP. This procedure is complete.

DLP-029
Test OC12 Protection Switching

Purpose

Provide procedures for testing OC12 protection switching.

STEP	PROCEDURE

1 Determine the facility protection switching mode at both ends of the OC12 span:

a. In the scope pane, expand Facility and select OC12.

b. In the result pane, right-click OC12 facility being tested to display a context menu.

c. From the context menu, select **Task>Provision>Switch** to display a work view.

d. Verify parameters are provisioned per company requirements.

NOTE: *The switch direction parameter must be set to the same value (unidirectional or bidirectional) at both ends of the OC12 facility.*

e. If necessary, modify switching parameters.

f. On the toolbar, select Submit; then close work view.

2 Refer to Table A and select the test you want to perform; then go to the referenced step.

Table A. Protection Switching Choices

IF SWITCH DIRECTION IS...	AND YOU WANT TO PERFORM A...	THEN GO TO...
Unidirectional	Normal Switch	Step 3
	Fast Switch	Step 10
Bidirectional	Normal Switch	Step 19
	Fast Switch	Step 26

Unidirectional (Normal)

3 Switch OC12 facility [DLP-515].

4 Verify that the switch took place by observing ACT (active) LEDs on the HIF/LIF and Service Condition column.

5 Did switch take place?

If yes, go to step 7.
If no, then go to step 6.

6 Verify that there are no alarms on the OC12 facility. If necessary, replace HIF/LIF plug-ins [DLP-101]; then repeat procedure.

7 Release facility protection switch [DLP-545].

NOTE: *If switching mode is revertive, the A-side is always the working side, and the B-side is the standby side. When the protection switch is released, the facility returns to the A side.*

If switching mode is nonrevertive, the active side becomes the working side when the protection switch is released. The facility does not return to previous side.

8 Log on to the NE that terminates the OC12 span and repeat steps 3 through 7.

9 STOP. This procedure is complete.

Unidirectional (Fast)

10 Allow fast facility protection (FFP) switch [DLP-573].

11 Switch OC12 facility [DLP-515].

12 Repeat switch (step 11) several times.

13 Retrieve PM registers [DLP-517] and verify that the PSC, Protection Switch Count, register recorded all the switches.

14 Did all the switches take place?

If yes, go to step 16.
If no, then go to step 15.

15 Verify there are no alarms on the OC12 facility. If necessary, replace HIF/LIF plug-ins [DLP-101]; then repeat procedure.

16 Release facility protection switch [DLP-545].

NOTE: *If switching mode is revertive, facility returns to the A-side. If nonrevertive, facility does not return to A-side.*

17 Log on to the NE that terminates the OC12 span and repeat steps 11 through 16.

18 STOP. This procedure is complete.

Bidirectional (Normal)

19 **NOTE:** *Observe that switching takes place at both NEs.*

Log on to the NE that terminates the OC12 span [DLP-117] if a craftsperson is not there to observe events.

20 At one NE only, switch OC12 facility [DLP-515].

21 Verify that the switch took place at both ends by observing ACT (active) LEDs on the HIF/LIF and Service Condition column.

22 Did switch take place?

If yes, go to step 24.
If no, then go to step 23.

23 Verify that there are no alarms on the OC12 facility. If necessary, replace HIF/LIF plug-ins [DLP-101]; then repeat procedure.

24 Release facility protection switch [DLP-545].

NOTE: *If switching mode is revertive, facility returns to the A-side. If nonrevertive, facility does not return to A-side.*

25 STOP. This procedure is complete.

Bidirectional (Fast)

26 ***NOTE:*** *Observe that switching takes place at both NEs.*

Log on to the NE that terminates the OC12 span [DLP-117] if a craftsperson is not there to observe events.

27 Allow fast facility protection (FFP) switch [DLP-573].

28 At one NE only, switch OC12 facility [DLP-515].

29 Retrieve PM registers [DLP-517] at both NEs and verify that the PSC, Protection Switch Count, register recorded all the switches.

30 Did all the switches take place?

If yes, go to step 32.
If no, then go to step 31

31 Verify there are no alarms on the OC12 facility. If necessary, replace HIF/LIF plug-ins [DLP-101]; then repeat procedure.

32 Release facility protection switch [DLP-545].

NOTE: *If switching mode is revertive, facility returns to the A-side. If nonrevertive, facility does not return to A-side.*

33 STOP. This procedure is complete.

DLP-030
Test OC48 Loopbacks

Purpose

This procedure describes how to test OC48 loopbacks.

STEP	PROCEDURE

1 **CAUTION: Possibility of service interruption. Placing the OC48 facility in maintenance state causes a line AIS (alarm insertion signal) to be transmitted on the OC48 facility. If the facility is active, it causes a line switch in a linear configuration, a path switch in a ring configuration, or a BLSR switch in a BLSR configuration. This may interrupt service if a protection line or protecting path is not available.**

2 ***NOTE:*** *Loopbacks (facility or terminal) are not allowed while input synchronization messaging is enabled for the same facility. If necessary, edit the facility to disable input synchronization messaging.*

Place facility being looped in maintenance state:

a. In the scope pane, expand Facility and select OC48.

b. In the result pane, right-click OC48 being tested to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select Maintenance.

e. On the toolbar, select Submit; then close work view.

3 See Figure 1. Operate a loopback toward the NE (terminal):

a. In the scope pane, expand Facility and select OC48.

b. In the result pane, right-click OC48 being tested to display a context menu.

c. From context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From Loop Mode drop-down list, select Terminal.

e. On the toolbar, select Submit; then close work view.

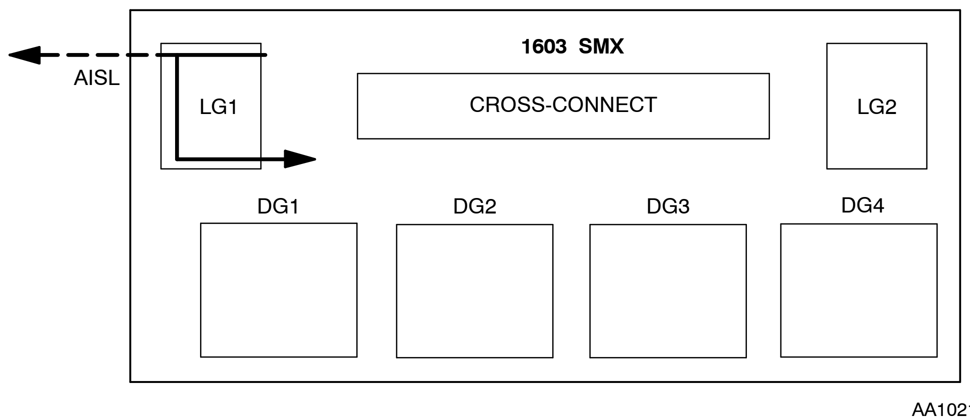


Figure 1. OC48 Loopback Toward Terminal (NE)

4 Verify the test signal is looped back to the sending end.

5 Release the loopback:

a. In the scope pane, expand Facility and select OC48.

b. In the result pane, right-click OC48 being tested to display a context menu.

c. From context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

6 See Figure 2. Operate a loopback toward the facility:

a. In the scope pane, expand Facility and select OC48.

b. In the result pane, right-click OC48 being tested to display a context menu.

c. From context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From Loop Mode drop-down list, select Facility:N,F.

e. On the toolbar, select Submit; then close work view.

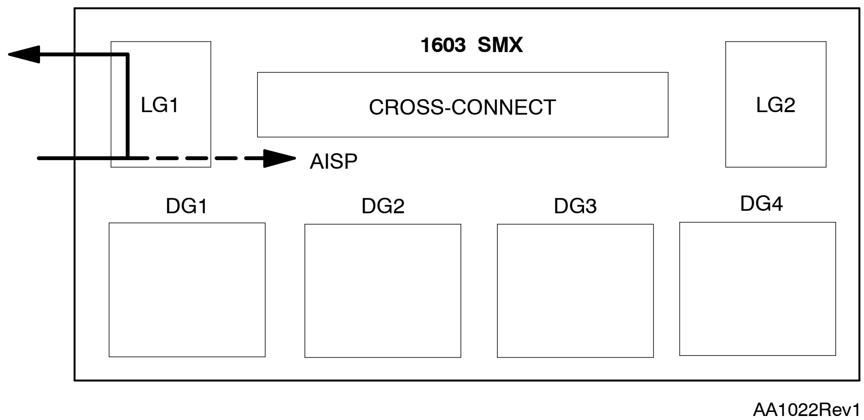


Figure 2. OC48 Loopback Toward Facility

7 Verify the test signal is looped back to the sending end.

8 Release the loopback:

a. In the scope pane, expand Facility and select OC48.

b. In the result pane, right-click OC48 being tested to display a context menu.

c. From context menu, select **Task>Operate>Loopbacks** to display a work view.

d. From Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

9 When loopback tests are completed, place port in required service state:

a. In the scope pane, expand Facility and select OC48.

b. In the result pane, right-click OC48 being returned to original service state to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select In Service or Memory Administration (as required).

e. On the toolbar, select Submit; then close work view.

10 STOP. This procedure is complete.

DLP-031
Test OC48 Protection Switching

Purpose

Provide procedures for testing OC48 protection switching.

STEP	PROCEDURE

1 Determine the facility protection switching mode at both ends of the OC48 span:

a. In the scope pane, expand Facility and select OC48.

b. In the result pane, right-click OC48 facility being tested to display a context menu.

c. From the context menu, select **Task>Provision>Switch** to display a work view.

d. Verify parameters are provisioned per company requirements.

NOTE: *The switch direction parameter must be set to the same value (unidirectional or bidirectional) at both ends of the OC48 facility.*

e. If necessary, modify switching parameters.

f. On the toolbar, select Submit; then close work view.

2 Refer to Table A and select the test you want to perform; then go to the referenced step.

Table A. Protection Switching Choices

IF SWITCH DIRECTION IS...	AND RING TYPE IS...	AND YOU WANT TO PERFORM A...	THEN GO TO...
Unidirectional	—	Normal Switch	Step 3
	—	Fast Switch	Step 10
Bidirectional	UPSR	Normal Switch	Step 19
	UPSR	Fast Switch	Step 26
	BLSR	Manual switch from working to protection	Step 34
	BLSR	Forced switch from working to protection	Step 41
	BLSR	Lockout of working channels at local NE	Step 48
	BLSR	Lockout of protection channels for entire ring	Step 55

Unidirectional (Normal)

3 Switch OC48 facility [DLP-515].

4 Verify the switch took place by observing ACT (active) LEDs on the HIF and Service Condition column.

5 Did switch take place?

If yes, go to step 7.
If no, then go to step 6.

6 Verify there are no alarms on the OC48 facility. If necessary, replace HIF plug-ins [DLP-101]; then repeat procedure from step 3.

7 Release the protection switch [DLP-545].

NOTE: *If switching mode is revertive, facility returns to the A-side. If nonrevertive, facility does not return to A-side.*

8 Log on to the NE that terminates the OC48 span and repeat steps 3 through 7.

9 STOP. This procedure is complete.

Unidirectional (Fast)

10 Allow fast facility protection (FFP) switch [DLP-573].

11 Switch OC48 facility [DLP-515].

12 Repeat switch (step 11) several times.

13 Retrieve PM registers [DLP-517] and verify that the PSC, Protection Switch Count, register recorded all the switches.

14 Did all the switches take place?

If yes, go to step 16.
If no, then go to step 15.

15 Verify there are no alarms on the OC48 facility. If necessary, replace HIF plug-ins [DLP-101]; then repeat procedure from step 11.

16 Release facility protection switch [DLP-545].

NOTE: *If switching mode is revertive, facility returns to the A-side. If nonrevertive, facility does not return to A-side.*

17 Log on to the Network Element (NE) that terminates the OC48 span and repeat steps 11 through 16.

18 STOP. This procedure is complete.

Bidirectional UPSR (Normal)

19 ***NOTE:*** *Observe that switching takes place at both NEs.*

Log on to the NE that terminates the OC48 span [DLP-117] if a craftsperson is not there to observe events.

20 Switch OC48 facility (only at one end):

a. In the scope pane, expand Facility and select OC48.

b. In the result pane, right-click OC48 facility being switched to display a context menu.

c. From the context menu, select **Task>Operate>Switch>APS** to display a work view.

d. Select active OC48.

e. In the Switch Mode region, select Manual radio button.

f. On the toolbar, select Submit.

21 Verify the switch took place by observing ACT (active) LEDs on the HIF and Primary State column.

22 Did switch take place?

If yes, go to step 24.
If no, then go to step 23.

23 Verify there are no alarms on the OC48 facility. If necessary, replace HIF plug-ins [DLP-101]; then repeat from step 20.

24 Release the protection switch [DLP-545].

NOTE: *If switching mode is revertive, facility returns to the A-side. If nonrevertive, facility does not return to A-side.*

25 STOP. This procedure is complete.

Bidirectional UPSR (Fast)

26 Allow fast facility protection (FFP) switch [DLP-573].

27 Switch OC48 facility [DLP-515].
(**Task>Operate>Switch>APS**)

NOTE: *Observe that switching takes place at both NEs.*

28 Repeat switch (step 27) several times.

29 Retrieve PM registers [DLP-517] and verify that the PSC, Protection Switch Count, register recorded all the switches.

30 Did all the switches take place?

If yes, go to step 32.
If no, then go to step 31.

31 Verify there are no alarms on the OC48 facility. If necessary, replace HIF plug-ins [DLP-101]; then repeat procedure from step 27.

32 Release facility protection switch [DLP-545].

NOTE: *If switching mode is revertive, facility returns to the A-side. If nonrevertive, facility does not return to A-side.*

33 STOP. This procedure is complete.

Manual Switch (BLSR)

34 Log on to the NE that terminates the OC48 span [DLP-117] if a craftsperson is not there to observe events.

35 Perform a manual switch from working channels to protection channels (BLSR):

a. In the scope pane, expand Facility and select OC48.

b. In the result pane, right-click OC48 facility being switched to display a context menu.

c. From the context menu, select **Task>Operate>Switch>BLSR** to display a work view.

d. Select active OC48.

e. In the Switch Mode region, select Manual radio button.

f. On the toolbar, select Submit.

36 Retrieve OC48 conditions and verify that MAN-RING was reported at both NEs.

37 Did manual switch occur?

If yes, go to step 39.
If no, then go to step 38.

38 Verify there are no alarms on the OC48 facility. If necessary, replace HIF plug-ins [DLP-101]; then repeat procedure from step 35.

39 Release manual switch [DLP-545].

NOTE: *If switching mode is revertive, the facility returns to the A-side. If nonrevertive, the facility does not return to A-side.*

40 STOP. This procedure is complete.

Forced Switch (BLSR)

41 Log on to the NE that terminates the OC48 span [DLP-117] if a craftsperson is not there to observe events.

42 Perform a forced switch from working channels to protection channels (BLSR):

a. In the scope pane, expand Facility and select OC48.

b. In the result pane, right-click OC48 facility being switched to display a context menu.

c. From the context menu, select **Task>Operate>Switch>BLSR** to display a work view.

d. Select active OC48.

e. In the Switch Mode region, select Forced radio button.

f. On the toolbar, select Submit.

43 Retrieve OC48 conditions and verify that FRCD-RING was reported at both NEs.

44 Did forced switch occur?

If yes, go to step 46.
If no, then go to step 45.

45 Verify there are no alarms on the OC48 facility. If necessary, replace HIF plug-ins [DLP-101]; then repeat procedure from step 42.

46 Release forced switch [DLP-545].

NOTE: *If switching mode is revertive, the facility returns to the A-side. If nonrevertive, the facility does not return to A-side.*

47 STOP. This procedure is complete.

Lockout of Working Channels (BLSR)

48 Log on to the NE that terminates the OC48 span [DLP-117] if a craftsperson is not there to observe events.

49 Perform a lockout of working channels at the local NE:

a. In the scope pane, expand Facility and select OC48.

b. In the result pane, right-click OC48 facility being switched to display a context menu.

c. From the context menu, select **Task>Operate>Switch>BLSR** to display a work view.

d. Select active OC48.

e. In the Switch Mode region, select Lockout Working Channels radio button.

f. On the toolbar, select Submit.

50 Retrieve OC48 conditions and verify that LOCKOUT-LOWR was reported at both NEs.

51 Did lockout occur?

If yes, go to step 53.
If no, then go to step 52.

52 Verify there are no alarms on the OC48 facility. If necessary, replace HIF plug-ins [DLP-101]; then repeat procedure from step 49.

53 Release lockout [DLP-545].

NOTE: *If switching mode is revertive, the facility returns to the A-side. If nonrevertive, the facility does not return to A-side.*

54 STOP. This procedure is complete.

Lockout of Protection Channels (BLSR)

55 Log on to the NE that terminates the OC48 span [DLP-117] if a craftsperson is not there to observe events.

56 Perform a lockout of protection channels for the entire ring:

a. In the scope pane, expand Facility and select OC48.

b. In the result pane, right-click OC48 facility being switched to display a context menu.

c. From the context menu, select **Task>Operate>Switch>BLSR** to display a work view.

d. Select active OC48.

e. In the Switch Mode region, select Lockout Protection All Spans radio button.

f. On the toolbar, select Submit.

57 Retrieve OC48 conditions and verify that LOCKOUT-LPS was reported.

58 Did lockout occur?

If yes, go to step 60.
If no, then go to step 59.

59 Verify there are no alarms on the OC48 facility. If necessary, replace HIF plug-ins [DLP-101]; then repeat procedure from step 56.

60 Release lockout [DLP-545].

NOTE: *If switching mode is revertive, the facility returns to the A-side. If nonrevertive, the facility does not return to A-side.*

61 STOP. This procedure is complete.

DLP-100
Retrieve Alarms/Conditions

Purpose

This procedure describes how to retrieve alarms and conditions for 1603 SMX entities.

STEP	PROCEDURE

1 Find the entity for which you want to retrieve alarms or conditions in Table A.

Table A. Retrieving Alarms/Conditions

IF YOU WANT TO RETRIEVE ALARMS/CONDITIONS FOR...	THEN GO TO...
NE (i.e., all current alarms)	Step 2
BLSR ring	Step 6
Common entities	Step 10
Plug-in units (i.e., COA, HIF, LIF, etc.)	Step 14
Facilities (i.e., OC3, OC12, EC1, etc.)	Step 19
IP Tunnel	Step 24
Paths (i.e., STS1, VT1.5, etc.)	Step 29
Ports (i.e., Craft 1, Craft 2, SE2A, etc.)	Step 34
Protocols (i.e., TADRMap, X.25, etc.)	Step 39
Synchronization entities (i.e., NE Sync, BITS Sync, or BITS)	Step 44
Customer defined alarms	Step 49

Retrieve All Current NE Alarms

2 In the scope pane, right-click NE name to display a context menu.

3 From the context menu, select **Monitor Alarms** to display a work view.

4 Record alarms/conditions listed on work view; then close work view.

5 STOP. This procedure is complete.

Retrieve BLSR Ring Alarms/Conditions

6 In the scope pane, expand BLSR and right-click BLSR Ring to display a context menu.

7 From the context menu, select **Monitor Alarms** or **Monitor Conditions** to display a work view.

8 Record alarms/conditions listed on work view; then close work view.

9 STOP. This procedure is complete.

Retrieve Common Alarms/Conditions

10 In the scope pane, right-click Common to display a context menu.

11 From the context menu, select **Monitor Alarms** or **Monitor Conditions** to display a work view.

12 Record alarms/conditions listed on work view; then close work view.

13 STOP. This procedure is complete.

Retrieve Equipment Alarms/Conditions

14 In the scope pane, expand Equipment.

15 Right-click equipment entity you want to check to display a context menu.

16 From the context menu, select **Monitor Alarms** or **Monitor Conditions** to display a work view.

17 Record alarms/conditions listed on work view; then close work view.

18 STOP. This procedure is complete.

Retrieve Facility Alarms/Conditions

19 In the scope pane, expand Facility.

20 Select and right-click the facility you want to check to display a context menu.

21 From the context menu, select **Monitor Alarms** or **Monitor Conditions** to display a work view.

22 Record alarms/conditions listed on work view; then close work view.

23 STOP. This procedure is complete.

Retrieve IP Tunnel Alarms/Conditions

24 In the scope pane, expand System.

25 Expand Network Feature; then select and right-click IP Tunnel to display a context menu.

26 From the context menu, select **Monitor Alarms** or **Monitor Conditions** to display a work view.

27 Record alarms/conditions listed on work view; then close work view.

28 STOP. This procedure is complete.

Retrieve Path Alarms/Conditions

29 In the scope pane, expand Facility; then expand the facility that contains the path you want to check.

30 Select and right-click the path you want to check to display a context menu.

31 From the context menu, select **Monitor Alarms** or **Monitor Conditions** to display a work view.

32 Record alarms listed on work view; then close work view.

33 STOP. This procedure is complete.

Retrieve Ports Alarms/Conditions

34 In the scope pane, expand System; then expand Ports.

35 Right-click Craft-Front, Craft-Rear, or SML to display a context menu.

36 From the context menu, select **Monitor Alarms** or **Monitor Conditions** to display a work view.

37 Record alarms/conditions listed on work view; then close work view.

38 STOP. This procedure is complete.

Retrieve Protocols Alarms/Conditions

39 In the scope pane, expand System; then expand Protocols.

40 Right-click the protocol (i.e, DCC-Lower Layer, TADRMap, X.25, etc.) that you want to retrieve.

41 From the context menu that is displayed, select **Monitor Alarms** or **Monitor Conditions** to display a work view.

42 Record alarms/conditions listed on work view; then close work view.

43 STOP. This procedure is complete.

Retrieve Synchronization Alarms/Conditions

44 In the scope pane, expand System; then expand Synchronization.

45 Right-click NE Sync, BITS Sync, or BITS to display a context menu.

46 From the context menu, select **Monitor Alarms** or **Monitor Conditions** to display a work view.

47 Record alarms/conditions listed on work view; then close work view.

48 STOP. This procedure is complete.

Retrieve Customer Defined Alarms/Conditions

49 In the scope pane, expand System; then expand Network Features.

50 Right-click Env Alarms to display a context menu.

51 From the context menu, select **Monitor Alarms** or **Monitor Conditions** to display a work view.

52 Record alarms/conditions listed on work view; then close work view.

53 STOP. This procedure is complete.

DLP-101
Replace Plug-in Units

Purpose

This procedure provides the steps to follow when replacing a faulty unit or a unit suspected of being faulty. Do not remove a unit that is providing service. This procedure assumes the replacement unit is not faulty.

General

This procedure assumes the automatic download feature is enabled. It is also assumed that, if the NE is equipped with a COA with expanded memory (COA603–610), the program backup has the correct version of software for the replacement unit. The NE reports a COM:PROGVER alarm if the program backup unit does not have the current version of the software loaded.

In this procedure, the unit being replaced and, if applicable, its associated facility, may be placed Out-of-Service for Maintenance activity state (OOS-MT) to prevent additional alarms. This is optional and per local procedure. Restore unit to In-Service (IS) after it is replaced and send faulty unit to the repair and return facility per local practice or refer to TNG-505.

Prerequisites

When replacing a plug-in unit, compare the equipment types. If the equipment types are different, be certain the replacement unit has the same software compatibility code.

STEP	PROCEDURE
1	**CAUTION: Possibility of service interruption. Replacing a unit may interrupt service if the wrong unit is removed or if unit removed is carrying traffic. Before unplugging any unit in a redundant configuration, wait at least 30 seconds if the other unit of the redundant pair was just plugged in.**
2	***WARNING: Possibility of damage to equipment. This equipment contains static-sensitive devices. Refer to DLP-518 for special handling instructions.***
3	**NOTE:** *If the unit to be replaced is non-optic, active, and redundant, switch the unit to standby before replacing. If the unit to be replaced is optic, active, and redundant, switch the active facility to standby before replacing the unit. If the unit being replaced is an A-side unit and revertive switching is enabled, a switch to the B-side unit reverts to the A-side unit after approximately two minutes (if the A-side unit is equipped and able to carry traffic). Therefore, unplug the unit being replaced within two minutes after entering switch command.*

Find the plug-in unit you want to replace in Table A, and go to the step referenced for the replacement procedure. Refer to Table B for plug-in software compatibility.

Table A. Plug-in Replacement Units

IF UNIT BEING REPLACED IS...	THEN GO TO...
CCM	Step 4
CLK	Step 11
COA	Step 17
DMI	Step 26
HIF (linear configuration)	Step 33
HIF (ring configuration — UPSR or BLSR)	Step 45
LDR (w/LIF20x or LIF30x)	Step 63
LDR (w/LIF50x, 601 or 701)	Step 68
LDR501 (working)	Step 73
LDR501 (protection)	Step 81
LIF20x/30x/50x/601/701/D01	Step 26
LIF40x/A0x (OC3/OC12 drop)	Step 86
LIFF01	Step 98
LIF901 (Ethernet LAN)	Step 111
LIFG01 (Gigabit Ethernet)	Step 124
NEP	Step 131
PWR	Step 139
VTG (working)	Step 143
VTG (protection)	Step 174

Table B. Plug-in Replacement Compatibility Based on Software Compatibility Code

PLUG-IN UNIT NAME	UNIT MNEMONIC (EQUIPMENT CODE)	SOFTWARE COMPATIBILITY CODE
Cross-Connect Matrix	CCM101	CCM101
	CCM201	CCM201
Clock	CLK202	CLK202
	CLK203	CLK202
Craft, Orderwire and Alarm	COA601, 603, 605	COA601
	COA602, 604, 606	COA602
	COA607	COA607
	COA608	COA608
	COA609	COA601
	COA610	COA602
Drop Module Interface	DMI102	DMI102
	DMI301	DMI301
High Speed Interface (OC3)	HIFB0x, HIFC0x	HIFB01
High Speed Interface (OC12)	HIF601, 602, 606	HIF601
	HIF603, 604, 605, 607	HIF603
	HIF701, 702	HIF601
	HIF703, 704, 705, 706	HIF603
	HIF901, 902, 905, 906	HIF601
	HIF903, 904, 907, 908	HIF603
	HIFA01, A02, A05, A06, A07	HIF601
	HIFA03, A04, A08, A09	HIF603
High Speed Interface (OC48)	HIFF01, F02, F03, F04	HIFF01
	HIFH0x	HIFF01
	HIFJAx, JBx, JCx, JDx, JEx, JFx	HIFF01
Line Driver/Receiver	LDR101	LDR101
	LDR201	LDR201
	LDR301	LDR301
	LDR501	LDR501

Table B. Plug-in Replacement Compatibility Based on Software Compatibility Code (cont)

PLUG-IN UNIT NAME	UNIT MNEMONIC (EQUIPMENT CODE)	SOFTWARE COMPATIBILITY CODE
Low Speed Interface (DS3, EC1, STS, and USRLAN)	LIF201, 202	LIF201
	LIF301, 302	LIF301
	LIF501, 502	LIF501
	LIF601, 602	LIF601
	LIF701	LIF701
	LIF901	LIF901
	LIFD01	LIFD01
	LIFG01	LIFG01
Low Speed Interface (OC3)	LIF401, 402, 403	LIF401
	LIF404, 405, 406, 407	LIF404
	LIFF01	LIFF01
Low Speed Interface (OC12)	LIFA01, A02, A03, A04, H01, H02, H03, H04	LIFA01
Network Element Processor	NEP602 (w/LAN)	NEP602
	NEP603 (w/o LAN)	NEP603
Power Converter/Supply	PWRA01, PWRB01	PWRA01
Virtual Tributary Group	VTG101*	VTG101
	VTG102*	VTG102
	VTG301	VTG301

* *VTG101 and VTG102 are software compatible units for replacement purposes. Refer to VTG replacement procedure for details.*

Replace CCM Unit

4 If CCM being replaced is active and redundant, switch active CCM to standby:

a. In the scope pane, expand Equipment and select CCM.

b. In the result pane, right-click active CCM to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open a work view.

d. Select active CCM.

e. In the Switch Mode region, select Forced radio button.

f. On the toolbar, select Submit; then close work view.

5 Replace CCM with spare.

6 Is MEA alarm being reported?

If yes, go to step 7.
If no, go to step 8.

7 Change the Equipment Type in database to agree with the replacement unit:

a. In the scope pane, expand Equipment and select CCM.

b. In the result pane, right-click CCM to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Equipment Type drop-down list, select the unit name that matches the replacement unit (unit name appears on faceplate).

e. On the toolbar, select Submit; then close work view.

8 Was software copied to replacement CCM?

NOTE: *If another unit of the same plug-in type is equipped, or COA program backup is used, software is automatically copied to the replacement unit. The ACT LED on the unit flashes to indicate the automatic download is in progress.*

If software was not copied, go to step 9.
If software was copied, STOP. This procedure is complete.

9 Manually download software from PC to CCM [DLP-566].

10 STOP. This procedure is complete.

Replace CLK Unit

11 **CAUTION: Possibility of service interruption. If provided, BITS input/output is interrupted on SYNCPRI if CLK-A is removed and on SYNCSEC if CLK-B is removed.**

12 If CLK being replaced is active and redundant, switch active CLK to standby:

a. In the scope pane, expand Equipment and select CLK.

b. In the result pane, right-click active CLK to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open a work view.

d. Select active CLK.

e. In the Switch Mode region, select Forced radio button.

f. On the toolbar, select Submit; then close work view.

13 Are DMI102 and LIF20x/30x active on the same side as CLK being replaced.

If yes, go to step 14.
If no, go to step 15.

14 Switch active DMI102 and LIF20x/30x to standby:

a. In the scope pane, expand Equipment and select DMI (or LIF).

b. In the result pane, right-click active DMI (or LIF) to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open a work view.

d. Select active CLK.

e. In the Switch Mode region, select Forced radio button.

f. On the toolbar, select Submit; then close work view.

15 Replace CLK with spare unit.

16 STOP. This procedure is complete.

Replace COA Unit

17 **CAUTION: Possibility of service interruption. Do not remove NEP, initialize system (cold- or warm-start), or remove power while COA is being replaced. If you do, the provisioning database will be lost.**

18 Replace COA with a spare unit.

19 After replacing COA, is either a MEMVER or MEMDIF alarm reported?

If yes, go to step 20.
If no, STOP. This procedure is complete.

20 Copy database from NEP to COA (working to primary) [DLP-538].

21 After copying database, is a COM-PROGVER alarm reported?

If yes, go to step 22
If no, STOP. This procedure is complete.

22 Try to silence alarm by downloading system software matching current NEP version to the COA. To download from a PC, refer to DLP-566; to download from a remote NE, refer to DLP-569.

23 After downloading system software from PC or remote NE, is COM-PROGVER alarm silenced?

If yes, STOP. This procedure is complete.
If no, go to step 24.

24 Silence alarm by setting COM PROGVER, Software Program Version Error attribute, to Not Reported:

a. In the scope pane, select Common.

b. In the result pane, right-click COM to display a context menu.

c. From the context menu, select **Task>Provision>Alarm Conditions** to open a work view.

d. From the Condition drop-down list, select PROGVER.

e. From Active or A Side Notification Code drop-down list, select Not Reported.

f. On the toolbar, select Submit; then close work view.

25 STOP. This procedure is complete.

Replace DMI/LIF20x, 30x, 50x, 601, 701, D01

26 If unit being replaced is active and redundant, switch active unit to standby:

a. In the scope pane, expand Equipment and select DMI or LIF.

b. In the result pane, right-click active unit to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open a work view.

d. Select active unit.

e. In the Switch Mode region, select Forced radio button.

f. On the toolbar, select Submit; then close work view.

27 Replace unit with spare.

28 Is MEA alarm being reported?

If yes, go to step 29.
If no, go to step 30.

29 Change the Equipment Type in database to agree with the replacement unit:

a. In the scope pane, expand Equipment and select DMI or LIF.

b. In the result pane, right-click alarmed unit to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Equipment Type drop-down list, select the unit name that matches the replacement unit (unit name appears on faceplate).

e. On the toolbar, select Submit; then close work view.

30 Was software copied to replacement unit?

NOTE: *If another unit of the same plug-in type is equipped, or COA program backup is used, software is automatically copied to the replacement unit. The ACT LED on the unit flashes to indicate the automatic download is in progress.*

If software was not copied, go to step 31.
If software was copied, STOP. This procedure is complete.

31 Manually download software from PC to DMI/LIF [DLP-566].

32 STOP. This procedure is complete.

Replace HIF Unit (Linear Configuration)

33 If unit being replaced is active and redundant, switch active facility connected to unit to standby:

NOTE: *If revertive switching is enabled, use Forced switch option.*

a. In the scope pane, expand Facility and select OCn.

b. In the result pane, right-click facility being switched to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open a work view.

d. Select active facility.

e. In the Switch Mode region, select Forced radio button.

f. On the toolbar, select Submit; then close work view.

34 Is unidirectional protection switching being used?

If yes, go to step 35.
If no, go to step 38.

35 Use remote logon and determine if the far-end NE is receiving on the side to be removed:

a. In the scope pane, expand Facility and select OCn.

b. In the result pane, note the service state of OCn on side being removed.

36 Is the far-end NE receiving on the side to be removed?

If yes, go to step 37.
If no, go to step 38.

37 Switch far-end side with FRCD option, if revertive switching is used:

a. In the scope pane, expand Facility and select OCn.

b. In the result pane, right-click facility being switched to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open a work view.

d. Select active facility.

e. In the Switch Mode region, select Forced radio button.

f. On the toolbar, select Submit; then close work view.

38 Replace HIF with spare.

39 Is MEA alarm being reported?

If yes, go to step 40.
If no, go to step 41.

40 Change the provisioning to reflect the equipment type and compatibility code of the replacement unit:

NOTE: *If replacing an HIF601 compatible unit with an HIF603 compatible unit, or vice versa, both the equipment type and compatibility code must be modified at the same time. If replacing an HIF603 compatible unit with an HIF601 compatible unit, STS1 provisioning may also require modification.*

a. In the scope pane, expand Equipment and select HIF.

b. In the result pane, right-click alarmed unit to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Equipment Type drop-down list, select the unit name that matches the replacement unit (unit name appears on faceplate).

e. From the Compatibility Code drop-down list, select the compatibility code that matches the compatibility code of the replacement unit.

f. On the toolbar, select Submit; then close work view.

41 Was software copied to replacement HIF?

NOTE: *If another unit of the same plug-in type is equipped, or COA program backup is used, software is automatically copied to the replacement unit. The ACT LED on the unit flashes to indicate the automatic download is in progress.*

If software was not copied, go to step 42.
If software was copied, go to step 43.

42 Manually download software from PC to HIF [DLP-566].

43 If necessary, release OC3/OC12/OC48 protection switch at near end and far end:

a. In the scope pane, expand Facility and select OC3, OC12, or OC48.

b. In the result pane, right-click facility being switched to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open a work view.

d. Select active facility.

e. In the Switch Mode region, select Release radio button.

f. On the toolbar, select Submit; then close work view.

44 STOP. This procedure is complete.

Replace HIF Unit (BLSR or UPSR Ring)

45 **CAUTION: Possibility of service interruption. Unplugging the HIF removes a segment of the ring paths from the network and could cause service interruptions if there are other faults in the network that deny ring path switching. Take every precaution to ensure the HIF being removed is faulty or that its removal will not cause service interruptions. See Figure 1 for a typical ring network.**

46 ***NOTE:*** *Steps 46 to 55 ensure there are no preexisting conditions in the ring network that would not allow it to carry traffic when the HIF unit is removed.*

At each NE, verify there are no equipment failures (except for the HIF being replaced). Resolve any service-affecting alarms before continuing.

47 At each OCn interface in the network, except the one terminating the span from the HIF being replaced (see circled interfaces in Figure 1), verify there are no service-affecting alarms. Look for the following conditions: LOS, LOF, BERL-LT or BERL-HT. If found, resolve these alarms before continuing.

48 Check the ring for PROTNA and PATHSEL alarms. If either of these alarms exist, and they are not associated with the failed HIF, resolve the alarm(s) before continuing.

49 Is HIF being replaced in a BLSR ring or a UPSR ring with no BLSR NEs?

If BLSR ring go to step 50.
If UPSR ring, go to step 51.

50 Check the ring for BLSR alarms. If any BLSR alarms exist that are not associated with the HIF being replaced, resolve the alarm(s) before continuing.

51 At each NE, verify there are no path forced-level switches in effect (FRCD or LOCKOUT conditions in a UPSR ring or FRCD-RING, LOCKOUT-LOWR, or LOCKOUT-LPS in a BLSR ring):

52 Were any forced or locked out switches found?

If yes, go to step 53.
If no, go to step 54.

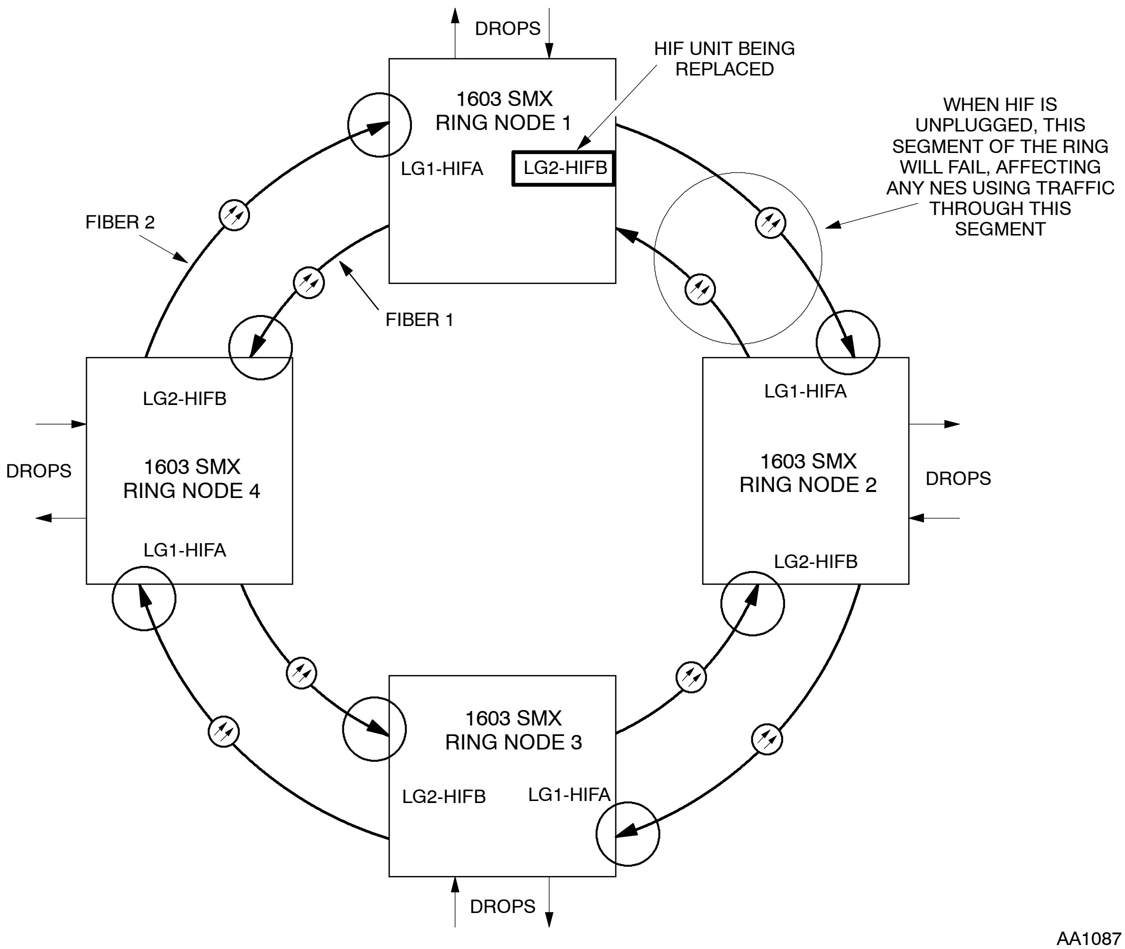


Figure 1. Replacing HIF Unit in a UPSR/BLSR Ring Network

53 Determine the reason for the forced or lockout condition; then release the forced or locked out switches to allow path selectors to switch away from the HIF being removed:

a. In the scope pane, expand Facility; then expand the type of facility that is carrying the path being released and select the path (i.e., STS1, STS3c, VT1, etc.).

b. In the result pane, right-click path being released to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open a work view.

d. Select active path.

e. In the Switch Mode region, select Release radio button.

f. On the toolbar, select Submit; then close work view.

54 At ring node 1, or where HIF unit is being replaced, switch ring traffic away from the unit. (See Figure 1.)

55 Place OCn facility in maintenance state for HIF being replaced (doing this sends AIS on ring to switch ring paths away from HIF):

a. In the scope pane, expand Facility and select OCn.

b. In the result pane, right-click facility being placed in maintenance state to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Service State drop-down list, select Maintenance.

e. On the toolbar, select Submit; then close work view.

56 Replace HIF with spare unit.

57 Is MEA alarm being reported?

If yes, go to step 58.
If no, go to step 59.

58 Change the provisioning to reflect the equipment type and compatibility code of the replacement unit:

NOTE: *If replacing an HIF601 compatible unit with an HIF603 compatible unit, or vice versa, both the equipment type and compatibility code must be modified at the same time. If replacing an HIF603 compatible unit with an HIF601 compatible unit, STS1 provisioning may also require modification.*

a. In the scope pane, expand Equipment and select HIF.

b. In the result pane, right-click alarmed unit to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Equipment Type drop-down list, select the unit name that matches the replacement unit (unit name appears on faceplate).

e. From the Compatibility Code drop-down list, select the compatibility code that matches the compatibility code of the replacement unit.

f. On the toolbar, select Submit; then close work view.

59 Was software copied to replacement unit?

NOTE: *If another unit of the same plug-in type is equipped, or COA program backup unit is used, software is automatically copied to the replacement unit. The ACT LED on the unit flashes to indicate the automatic download is in progress.*

If software was not copied, go to step 60.
If software was copied, go to step 61.

60 Manually download software from PC to HIF [DLP-566].

61 Place OCn facility back in-service:

a. In the scope pane, expand Facility and select OCn.

b. In the result pane, right-click facility being placed back in-service to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Service State drop-down list, select In Service.

e. On the toolbar, select Submit; then close work view.

62 STOP. This procedure is complete.

Replace LDR in Drop Group Containing LIF20x or LIF30x Unit

This procedure assumes LIF/LDR are redundant.

63 Switch active LIF to standby:

NOTE: *When LIF20x or LIF30x units are switched, the LDRs also switch, i.e., LDR-A is active when LIF-A is active, and LDR-B is active when LIF-B is active.*

a. In the scope pane, expand Equipment and select LIF.

b. In the result pane, right-click active LIF associated with LDR being replaced to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open an Operate Switch work view.

d. In Equipment region, select active LIF.

e. In the Switch Mode region, select Manual radio button.

f. On the toolbar, select Submit; then close work view.

64 Replace LDR with spare unit.

65 After replacing LDR, is MEA alarm being reported?

If yes, go to step 66.
If no, STOP. This procedure is complete.

66 Change the provisioning to reflect the equipment type of the replacement unit:

a. In the scope pane, expand Equipment and select LDR.

b. In the result pane, right-click alarmed unit to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Equipment Type drop-down list, select the unit name that matches the replacement unit (unit name appears on faceplate).

e. On the toolbar, select Submit; then close work view.

67 STOP. This procedure is complete.

Replace LDR in Drop Group Containing LIF50x, 601, or 701 Unit

NOTE: *This procedure assumes LIF/LDR are redundant.*

68 Switch active LDR to standby:

a. In the scope pane, expand Equipment and select LDR.

b. In the result pane, right-click active LDR being replaced to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open an Operate Switch work view.

d. In Equipment region, select active LDR.

e. In the Switch Mode region, select Manual radio button.

f. On the toolbar, select Submit; then close work view.

69 Replace LDR with spare unit.

70 After replacing LDR, is MEA alarm being reported?

If yes, go to step 71.
If no, STOP. This procedure is complete.

71 Change the provisioning to reflect the equipment type of the replacement unit:

a. In the scope pane, expand Equipment and select LDR.

b. In the result pane, right-click alarmed unit to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Equipment Type drop-down list, select the unit name that matches the replacement unit (unit name appears on faceplate).

e. On the toolbar, select Submit; then close work view.

72 STOP. This procedure is complete.

Replace LDR501

73 Retrieve LDR501 switching status:

a. In the scope pane, expand Equipment and select LDR.

b. In the result pane, note Secondary State status of the LDR501 being replaced (DGx-GRPy-LDR-1...3).

74 Is LDR501 being replaced active (ACT) or standby (STBY)?

If Active, go to step 75.
If Standby, go to step 77.

75 Inhibit automatic switching to working unit:

a. In the scope pane, expand Equipment and select LDR.

b. In the result pane, right-click LDR being replaced to display a context menu.

c. From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.

d. From Sw to Wkg drop-down list, select Inhibit.

e. On the toolbar, select Submit; then close work view.

76 Switch to protection LDR:

a. In the result pane, right-click LDR being replaced to display a context menu.

b. From the context menu, select **Task>Operate>Switch** to open a work view.

c. In the Equipment region, select LDR to be switched.

d. In the Switch Mode region, select Manual radio button.

e. On the toolbar, select Submit; then close work view.

77 Remove LDR501 and replace it with a spare LDR501 unit.

78 Was switching inhibited?

If yes, go to step 79.
If no, go to step 80.

79 Allow automatic switching to working unit:

a. In the result pane, right-click LDR just replaced to display a context menu.

b. From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.

c. From Sw to Wkg drop-down list, select Allow.

d. On the toolbar, select Submit; then close work view.

80 STOP. This procedure is complete.

Replace Protection LDR Unit

81 Retrieve LDR switching status:

a. In the scope pane, expand Equipment and select LDR.

b. In the result pane, note Secondary State status of the protection LDR501 (DGx-GRPy-LDR-P).

82 Is protection LDR501 Active (ACT) or Standby (STBY)?

NOTE: *If the protection LDR501 is active, the PSA LED is lighted green.*

If Active, go to step 83.
If Standby, go to step 84.

83 ***NOTE:*** *The protection LDR501 is actively protecting another LDR501 unit and should not be replaced until a working unit is available.*

Resolve other problems with working LDR501s before replacing protection LDR.

84 Remove LDR501 and replace with a spare LDR501 unit.

85 STOP. This procedure is complete.

Replace LIF40x/LIFA0x (OC3/OC12 drop)

86 If LIF unit being replaced is active and redundant, switch active facility connected to unit to standby:

NOTE: *Green LED on unit is on when unit is active.*

a. In the scope pane, expand Facility and select OCn.

b. In the result pane, right-click OCn facility being switched to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open a work view.

d. Select active facility.

e. In the Switch Mode region, select Forced radio button.

f. On the toolbar, select Submit; then close work view.

87 Is unidirectional protection switching being used?

If yes, go to step 88.
If no, go to step 91.

88 Use remote logon to determine if the far-end NE is receiving on the side to be removed:

a. In the scope pane, expand Facility and select OC3 or OC12.

b. In the result pane, note the primary state of the facility on the side being removed.

89 Is the far-end NE receiving on the side to be removed?

If yes, go to step 90
If no, go to step 91.

90 Switch far-end side:

a. In the scope pane, expand Facility and select OCn.

b. In the result pane, right-click OCn facility being switched to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open a work view.

d. Select active facility.

e. In the Switch Mode region, select Forced radio button.

f. On the toolbar, select Submit; then close work view.

91 Replace unit with spare.

92 Is MEA alarm being reported?

If yes, go to step 93.
If no, go to step 94.

93 Change the provisioning to reflect the equipment type of the replacement unit:

a. In the scope pane, expand Equipment and select LIF.

b. In the result pane, right-click alarmed unit to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Equipment Type drop-down list, select the unit name that matches the replacement unit (unit name appears on faceplate).

e. On the toolbar, select Submit; then close work view.

94 Was software copied to replacement unit?

NOTE: *If another unit of the same plug-in type is equipped, or COA program backup unit is used, software is automatically copied to the replacement unit. The ACT LED on the unit flashes to indicate the automatic download is in progress.*

If software was not copied, go to step 95.
If software was copied, go to step 96.

95 Manually download software from PC to LIF [DLP-566].

96 If necessary, release protection switch at near end and at far end.

97 STOP. This procedure is complete.

Replace LIFF01 Unit (OC3 drop)

98 If LIFF01 unit being replaced is active and redundant, switch active OC3 facilities connected to unit to standby:

NOTE: *All four OC3 facilities will be switched simultaneously to the redundant LIF unit.*

a. In the scope pane, expand Facility and select OC3.

b. In the result pane, right-click OC3 facility being switched to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open a work view.

d. Select active facility.

e. In the Switch Mode region, select Forced radio button.

f. On the toolbar, select Submit; then close work view.

99 Is unidirectional protection switching being used on any of the OC3s?

If yes, go to step 100.
If no, go to step 104.

100 Use remote logon to determine if far-end NE is receiving on side to be removed:

a. In the scope pane, expand Facility and select OC3.

b. In the result pane, note primary state of the facility on side being removed.

101 Is the far-end NE receiving on side to be removed?

If yes, go to step 102.
If no, go to step 104.

102 Switch far-end side:

a. In the scope pane, expand Facility and select OC3.

b. In the result pane, right-click OC3 facility being switched to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open a work view.

d. Select active facility.

e. In the Switch Mode region, select Forced radio button.

f. On the toolbar, select Submit; then close work view.

103 Repeat from step 100 for each OC3 facility on the LIFF01; then go to step 104.

104 Replace unit with spare. (Press retaining clips to remove fiber. When removing fibers it is possible for the protective fiber boots to slip down. If this happens, slip boots into properly dressed position when reconnecting fibers.)

105 Is MEA alarm being reported?

If yes, go to step 106.
If no, go to step 107.

106 Change the provisioning to reflect the equipment type of the replacement unit:

a. In the scope pane, expand Equipment and select LIF.

b. In the result pane, right-click alarmed unit to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Equipment Type drop-down list, select the unit name that matches the replacement unit (unit name appears on faceplate).

e. On the toolbar, select Submit; then close work view.

107 Was software copied to replacement unit?

NOTE: *If another unit of the same plug-in type is equipped, or COA program backup unit is used, software is automatically copied to the replacement unit. The ACT LED on the unit flashes to indicate the automatic download is in progress.*

If software was not copied, go to step 108.
If software was copied, go to step 109.

108 Manually download software from PC to LIF [DLP-566].

109 If necessary, release protection switch at near end and at far end.

110 STOP. This procedure is complete.

Replace LIF901 (Ethernet LAN)

111 **CAUTION: Possibility of service interruption. Replacing LIF901 unit causes loss of service until the new unit is equipped and downloaded with the correct software and firmware.**

112 Replace unit with spare.

113 Was software copied to replacement unit?

NOTE: *Software is automatically copied to the replacement unit if the following conditions are met: the Auto Download Feature is allowed and another unit of the same plug-in type is equipped, or a COA program backup unit is used. While the software is being copied, the ACT LED on the LIF unit flashes to indicate the download is in progress.*

If no, go to step 114.
If yes, go to step 115.

114 Manually download software from PC to LIF [DLP-566].

115 Was a FWMJVER or FWMNVER alarm reported?

If FWMJVER, go to step 117.
If FWMNVER, go to TAP-021 to clear alarm.
If no alarms, go to step 116.

116 STOP. This procedure is complete.

117 ***NOTE:*** *Data is stored on the LIF901 unit in two forms: system software and firmware. The system software is loaded into standard memory on the LIF901 like software for other 1603 SMX units, either automatically from the COA or manually. The firmware resides in flash memory on the LAN portion of the LIF901. A copy of the firmware is embedded in the system software so the firmware can be overwritten in the field.*

An FWMJVER alarm indicates that the major version number of the firmware image embedded in the system software is different than the major version number of the firmware on the LAN portion of the LIF901 unit. To clear the alarm, the in use firmware must be overwritten.

There are two ways to overwrite the in use firmware: 1) allow automatic download of LAN firmware or 2) manually download firmware.

Do you want to allow automatic downloading of LAN firmware or manually download firmware?

If you want to allow automatic download, go to step 118.
If you want to do a manual download, go to step 119.

118 Enable automatic download of LAN firmware:

a. In the scope pane, expand System; then expand General and select Global Settings.

b. In the result pane, right-click Global Settings to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. In NE Allow/Inhibit region, select Allow from Auto Download ATM LAN drop-down list

e. On toolbar, select Submit; then close work view.

119 Manually download firmware [DLP-533].

120 Retrieve alarms [DLP-100].

121 Did alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 122.

122 Contact Alcatel Customer Support [TNG-505].

123 STOP. This procedure is complete.

Replace LIFG01 (Gigabit Ethernet)

124 **CAUTION: Possibility of service interruption. Since LIFG01 units are non-redundant, replacing an LIFG01 causes loss of service until the new unit is equipped and downloaded with the correct software.**

125 Disconnect cables from unit.

126 Remove and replace LIFG01 unit.

127 Was software copied to replacement unit?

NOTE: *Software is automatically copied to the replacement unit if the Auto Download Feature is allowed. While the software is being copied, the ACT LED on the LIF unit flashes to indicate the download is in progress.*

If no, go to step 128.
If yes, go to step 129.

128 Manually download software from PC to LIF [DLP-566].

129 Reconnect cables to LIFG01 unit.

130 STOP. This procedure is complete.

Replace NEP Unit

131 **CAUTION: Possibility of service interruption. Be certain to download or copy from program backup the same version of software the system is running. Do not clear a MEMVER or MEMDIFTRAN alarm (if present) by copying database from NEP to COA.**

132 ***NOTE:*** *When replacing an NEP, the software release downloaded on the replacement NEP should be the same as the software release the system is currently running. If the software releases are not the same, a COA MEMVER or MEMDIFTRAN alarm is reported.*

NOTE: *The contents of the Secondary database is lost when an NEP is removed.*

Replace unit with spare.

133 Does COA have current software in program backup?

If yes, NEP is automatically downloaded from program backup.
If no, go to step 134.

134 Is MEMVER or MEMDIFTRAN alarm being reported?

If yes, go to step 135.
If no, STOP. This procedure is complete.

135 Copy database from COA to NEP (primary to working) [DLP-538].

136 STOP. This procedure is complete.

137 Manually download current software from PC to NEP [DLP-566].

NOTE: *Provisioned database is automatically copied from COA.*

138 STOP. This procedure is complete.

Replace PWRA01 Unit

139 Remove alarmed PWR unit. Wait five seconds and reseat it.

140 Did PWR alarm clear?

If yes, STOP. This procedure is complete.
If no, go to step 141.

141 Replace PWR unit with spare.

142 STOP. This procedure is complete.

Replace Working VTG Unit

143 **CAUTION: Possibility of service interruption. If any of the four DS1s terminated by the VTG have an active loopback, removal of the VTG will interrupt service on all four DS1s.**

144 Retrieve service state of DS1s terminated by VTG:

a. In the scope pane, expand Facility and select DS1.

b. In the result pane, note the service state of DS1s terminated by VTG.

145 Are any of the four DS1s OOS-MT?

If yes, go to step 146.
If no, go to step 147.

146 Place DS1s in-service or OOS-MA.

147 Are there any active DS1 loopbacks on the VTG that is being replaced?

If yes, go to step 148.
If no, go to step 149.

148 Release loopback(s):

a. In the scope pane, expand Facility and select DS1.

b. In the result pane, right-click VTG being tested to display a context menu.

c. From the context menu, select **Task>Operate>Loopbacks** to open a work view.

d. From the Loop Mode drop-down list, select Clear.

e. On the toolbar, select Submit; then close work view.

149 Is unit being replaced by a VTG101, VTG102, or VTG301?

If VTG101, go to step 150.
If VTG102 or VTG301, go to step 163.

150 Retrieve VTG switching status:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click VTG being replaced to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. On the work view, note Secondary State status.

151 Is unit active?

If yes, go to step 152
If no, go to step 154.

152 Inhibit automatic switching to working unit:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click working VTG to display a context menu.

c. From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.

d. From Sw to Wkg drop-down list, select Inhibit.

e. On the toolbar, select Submit; then close work view.

153 Switch to protection unit:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click VTG carrying alarmed T1 to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open an Equipment Switch: VTG work view.

d. Select active VTG to be switched from.

e. In the Switch Mode region, select Manual radio button.

f. On the toolbar, select Submit; then close work view.

154 Remove VTG unit, but do not install replacement unit yet.

155 Is VTG101 being replaced with a VTG102 (or VTG301)?

If yes, go to step 156.
If no, go to step 159.

156 Change the provisioning to reflect the equipment type and compatibility code of the replacement unit:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click alarmed unit to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Equipment Type drop-down list, select the unit name that matches the replacement unit (unit name appears on faceplate).

e. From the Compatibility Code drop-down list, select the compatibility code that matches the compatibility code of the replacement unit.

f. On the toolbar, select Submit; then close work view.

157 Is a VTG301 unit being installed?

If yes, go to step 158.
If no, go to step 159.

158 Install a DMI301 unit.

159 Install replacement VTG unit.

160 Was switching inhibited?

If yes, go to step 161.
If no, STOP. This procedure is complete.

161 Allow automatic switching to working unit:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click working VTG to display a context menu.

c. From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.

d. From Sw to Wkg drop-down list, select Allow.

e. On the toolbar, select Submit; then close work view.

162 STOP. This procedure is complete.

163 Observe PSA LED on the VTG unit to be replaced.

NOTE: *If the LED is lighted, unit is active.*

164 Is unit active?

If yes, go to step 165.
If no, go to step 167.

165 Inhibit automatic switching to working unit:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click working VTG to display a context menu.

c. From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.

d. From Sw to Wkg drop-down list, select Inhibit.

e. On the toolbar, select Submit; then close work view.

166 Switch to protection unit:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click VTG carrying alarmed T1 to display a context menu.

c. From the context menu, select **Task>Operate>Switch** to open an Equipment Switch: VTG work view.

d. Select active VTG to be switched from.

e. In the Switch Mode region, select Manual radio button.

f. On the toolbar, select Submit; then close work view.

167 Remove VTG unit, but do not install replacement unit yet.

168 Is VTG102/VTG301 being replaced with a VTG101?

If yes, go to step 169.
If no, go to step 171.

169 Change the provisioning to reflect the equipment type and compatibility code of the replacement unit:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click alarmed unit to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Equipment Type drop-down list, select the unit name that matches the replacement unit (unit name appears on faceplate).

e. From the Compatibility Code drop-down list, select the compatibility code that matches the compatibility code of the replacement unit.

f. On the toolbar, select Submit; then close work view.

170 Install replacement VTG unit.

171 Was switching inhibited?

If yes, go to step 172.
If no, STOP. This procedure is complete.

172 Allow automatic switching to working unit:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click working VTG to display a context menu.

c. From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.

d. From Sw to Wkg drop-down list, select Allow.

e. On the toolbar, select Submit; then close work view.

173 STOP. This procedure is complete.

Replace Protection VTG Unit

174 Is unit being replacing a VTG101, VTG102, or VTG301?

If VTG101, go to step 175.
If VTG102 or VTG301, go to step 185.

175 Retrieve VTG switching status:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click protection VTG (DGx-VTG-P) to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. On the work view, note Secondary State.

176 Is Secondary State Active or Standby?

If Active, go to step 177.
If Standby, go to step 178.

177 Resolve other problems with working VTGs before replacing protection VTG.

178 Remove VTG unit but do not install replacement unit yet.

179 Is VTG101 being replaced with a VTG102 (or VTG301)?

If yes, go to step 180.
If no, go to step 183.

180 Change the provisioning to reflect the equipment type and compatibility code for the replacement unit:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click alarmed unit to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Equipment Type drop-down list, select the unit name that matches the replacement unit (unit name appears on faceplate).

e. From the Compatibility Code drop-down list, select the compatibility code that matches the compatibility code of the replacement unit.

f. On the toolbar, select Submit; then close work view.

181 IS a VTG301 unit being installed?

If yes, go to step 182.
If no, go to step 183.

182 Install a DMI301 unit.

183 Install replacement VTG unit.

184 STOP. This procedure is complete.

185 Observe PSA LED on the protection VTG unit.

NOTE: *If the LED is lighted, unit is active.*

186 Is protection unit active?

If yes, go to step 187.
If no, go to step 188.

187 Resolve other problems with working VTGs before replacing protection VTG.

188 Remove VTG unit, but do not install replacement unit yet.

189 Is VTG102/VTG301 being replaced with a VTG101?

If yes, go to step 190.
If no, go to step 191.

190 Change the provisioning to reflect the equipment type and compatibility code for the replacement unit:

a. In the scope pane, expand Equipment and select VTG.

b. In the result pane, right-click alarmed unit to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Equipment Type drop-down list, select the unit name that matches the replacement unit (unit name appears on faceplate).

e. From the Compatibility Code drop-down list, select the compatibility code that matches the compatibility code of the replacement unit.

f. On the toolbar, select Submit; then close work view.

191 Install replacement VTG unit.

192 STOP. This procedure is complete.

DLP-117
Log On/Log Off 1603 SMX Network Element (NE)

Purpose

This procedure describes how to log on and log off a 1603 SMX network element.

STEP	PROCEDURE
1	Do you want to log on or log off? If log on, go to step 2. If log off, go to step 16.
2	On your Windows desktop, double click the 1301 NMX icon. **NOTE:** *The 1301 NMX Shell window opens.*
3	On the 1301 NMX Shell window menu bar, select Communications; then select Connections from the Communications menu.
4	On the Connections dialog that opens, select New.
5	In the New Connection dialog that opens, enter a name for the connection in the Name field; select a Port type (i.e., Direct, LAN, or Modem); and select OK. **NOTE:** *The New Connections dialog box closes and the Connections dialog is redisplayed.*
6	On the Connections dialog, complete the connection settings (i.e., IP address, IP port, etc.); then select Connect. **NOTE:** *After communications are established, the 1301 NMX Explorer application window opens.*

Discover Network

7	**NOTE:** *The 1301 NMX Explorer application window is divided into two panes: a scope pane (left pane) and a result pane (right pane).* In the scope pane on the NMX Explorer application window, click the plus sign (+) to the left of My Network icon. **NOTE:** *The (+) sign changes to a minus sign (-) and Network List appears below My Network.*

8 Right-click Network List to display a context menu.

9 From the context menu, select **Create New NE List**.

10 Follow the instructions on each of the work views. When you get to the last work view, select, Yes, create/update subnetworks; then select Finish.

NOTE: *The newly discovered NEs are listed in the result pane.*

Log On

11 In the result pane, right-click the NE you want to log on to.

12 From the context menu that appears, select Logon.

13 On the Logon to NE dialog that opens, enter your User Name and Password; then select OK.

14 After you are logged on to an NE, right-click the NE and select Open from the context menu that appears. The 1603 SMX Application browser opens.

NOTE: *The 1603 SMX Application browser is divided into two panes: a scope pane (left pane) and a result pane (right pane). The scope pane is a directory tree that lists the various NE entities that you can access, e.g., equipment, facilities, paths, etc. The directory tree is expanded by selecting the plus sign (+) to the left of an item and collapsed by selecting the minus sign (-) that appears after an item has been expanded. Tasks are selected from context menus which are opened by right-clicking an item in the result pane.*

15 STOP. This procedure is complete.

Log Off

16 To log off, close the 1603 SMX Application browser.

17 In the result pane of the 1301 NMX Explorer application window, right-click the NE you are logged on to.

18 From the context menu that appears, select Logoff .

19 STOP. This procedure is complete.

DLP-128
Provision NE for Telecommunications Management Network

Purpose

This procedure describes how to provision a Network Element (NE) for Telecommunications Management Network (TMN).

General

This procedure assumes that the NE is turned up and connected to a Synchronous Optical Network (SONET) and no alarms are present.

This procedure describes how to provision the NE System ID (SID), the Network Service Access Point (NSAP) address, and the Open Systems Interconnection (OSI) communications stack to allow Embedded Operation Channel (EOC) communications with other NEs in the network. The EOC channel is required for remote log on, Customer-Defined Alarms and Controls (CDAC), remote alarms (CDAC and FEALM), Serial E2A, and 1301 NMX PC Domain applications.

The 1603 SMX provides the Autodiscovery feature that automatically discovers the NSAPs of the NEs in the same network. The NEs must be SONET NEs running 7-Layer stack software.

STEP	PROCEDURE

1 See Figure 1. From work order, obtain the following information for the NE being provisioned:

a. System Network Identification. – This is the NE name and can also be referred to as SID, TID and NETID. It can be 1...20 alphanumeric characters.

b. NSAP – Organization Identification (L3ORG parameter) (6 hexadecimal digits).

c. NSAP – Level 2 Routing Domain and Level 1 Routing Area identification (four hexadecimal digits each). Together these two make up the L3ROU parameter.

d. Intermediate System Routing Type: IS1 (*default*) or IS2 (L3ISTYPE parameter).

e. Facilities to be provisioned for EOC communications: Line Group 1, Line Group 2, Synchronous Maintenance Link (SML) port, and/or LAN port.

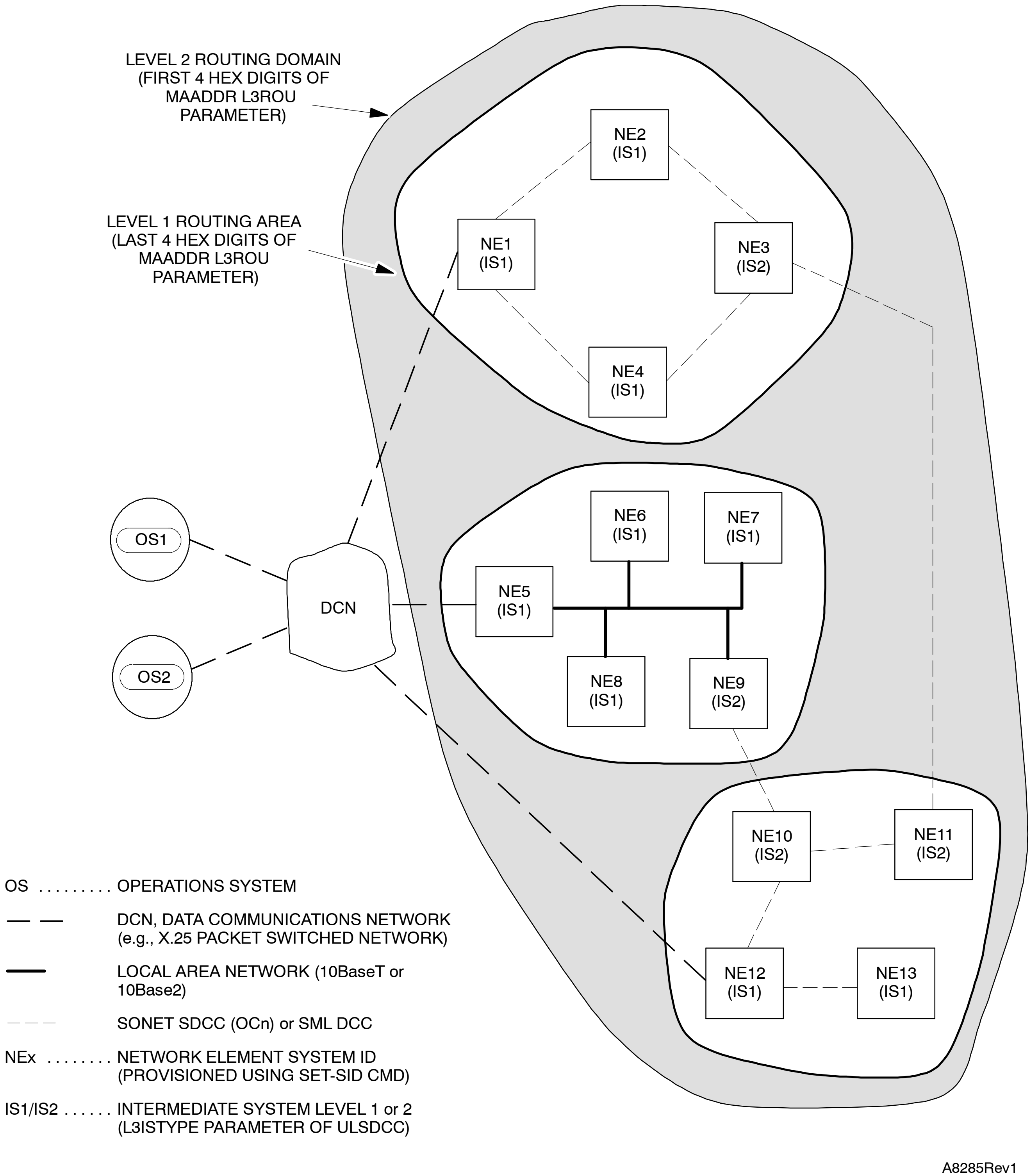


Figure 1. Example Telecommunications Management Network

2 If necessary, log on to the NE [DLP-117] and assign an NE name:

a. In the scope pane, expand System; then expand General and select NE Name.

b. In the result pane, right-click Name to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. On the work view, enter an NE name in the text box (1...20 alphanumeric characters).

e. On the toolbar, select Submit; then close work view.

3 ***NOTE:*** *The default Manual Area Address (MAADDR) can be used if the network will have only one L1 routing area. (Default values are Organization ID = 000000 and Area Address = 00000000.)*

Are NEs in network using default manual area addresses?

If yes, go to step 6.
If no, go to step 4.

4 Provision manual area address (MAADR) [DLP-129].

5 Log on to NE [DLP-117].

6 ***NOTE:*** *If the NE is connected to another NE in a different Level 1 (L1) routing area through a line group, SML, or LAN facility, select Yes (it requires the IS2 routing parameter).*

Is NE connected to one or more NEs outside its L1 Routing Area?

If yes, go to step 7.
If no, go to step 10.

7 Change DCC Upper Layer IS Routing parameter:

NOTE: *Select default parameters when entering command, except for parameter(s) listed. The values of the default parameters work in most network applications and should be used unless the work order specifies a different value.*

a. In the scope pane, expand System; then expand Protocols and select DCC-Upper Layer.

b. In the result pane, right-click DCC-Upper Layer to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. On the work view, note default values in Layer 3 Parameters and Layer 4 Parameters regions.

e. If required, select the IS Routing drop-down list (in the Layer 3 Parameters region) and select IS2.

f. Leave all other parameters at their default value unless instructed by work order.

g. On the toolbar, select Submit; then close work view.

8 Assign lower layer DCC for each line group or fiber drop group:

a. In the scope pane, expand Facility and select facility to be assigned.

b. In the result pane, right-click facility being assigned to display a context menu.

c. From the context menu, select **Task>Provision>DCC-Lower Layer** to display a work view.

d. On the work view, select Service State drop-down list and select In Service.

e. From the drop-down list under Side Role, select User Side at one end of the link and Network Side at the other end.

f. On the toolbar, select Submit; then close work view.

9 Repeat step 8 until all fiber facilities are assigned.

10 Is SML MAINT1 port to be used for EOC communications?

If yes, go to step 11.
If no, go to step 14.

11 Verify SML wiring is properly installed between NEs.

12 ***NOTE:*** *Select default parameters when entering command except for parameter(s) listed. The values of the default parameters work in most network applications and should be used unless work order specifies a different value.*

NOTE: *An SML LOS alarm is raised until SML is assigned at NE terminating the link.*

Assign SML MAINT1 port:

a. In the scope pane, expand System; then expand Ports and select SML.

b. In the result pane, right-click SML Port to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. In Equalization Distance column, use the spin box to select the distance to the terminating NE or cross-connect if provided.

e. Leave all other parameters at the default value unless specified by engineering work order.

f. On the toolbar, select Submit; then close work view.

13 ***NOTE:*** *An EOC alarm is raised until end-to-end connection is established.*

Assign Lower Layer of SML DCC:

a. In the scope pane, expand System; then expand Protocols and select DCC-Lower Layer.

b. In the result pane, right-click SML to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select In Service.

e. From the drop-down list under Side Role, select User Side at one end of the link and Network Side at the other end (see Figure 2).

f. Leave all other parameters at the default value unless specified by work order.

g. On the toolbar, select Submit; then close work view.

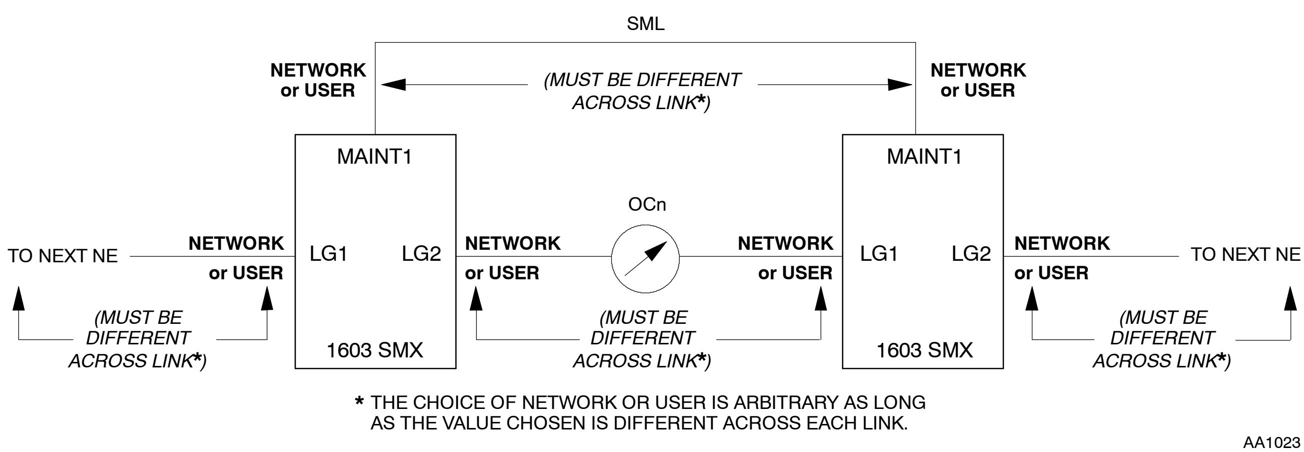


Figure 2. Example Layer 2 Side Role Parameter Entries

14 Is LAN to be used for EOC communications or TCP/IP gateway?

If yes, go to step 15.
If no, go to step 17.

15 Verify LAN wiring [DLP-020].

16 ***NOTE:*** *LAN CARLOS (loss of carrier) alarm is raised until carrier is detected.*

Assign LAN entity:

a. In the scope pane, expand System; then expand Protocols and select LAN.

b. In the result pane, right-click LAN to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. From the Service State drop-down list, select In Service.

e. From the LAN Type drop-down list, select either 10BASE2 or 10BASET.

NOTE: *Select 10BASE2 (10Base2) for a coaxial LAN interface, or 10BASET (10BaseT) for a twisted pair LAN interface. 10Base2 is the default.*

f. Leave other parameters at the default value unless specified by work order.

g. On the toolbar, select Submit; then close work view.

17 Retrieve system alarms:

a. In the scope pane, right-click NE name to display a context menu.

b. From the context menu, select **Monitor Alarms** to display current alarms.

18 If any alarms are reported, resolve them before continuing.

NOTE: *Each EOC link assigned must be terminated at another NE with proper provisioning before EOC alarms will retire.*

19 If associated facility alarms are present, resolve them before resolving EOC alarms. If alarms persist, refer to IXL-001 and locate the appropriate TAP to use to clear the alarm.

20 Enter PC Domain(s) this NE belongs to:

a. In the scope pane, expand System; then expand Network Features and select PC Domains.

b. In the result pane, right-click PC Domain being entered to display a context menu.

c. From the context menu, select **Provision Parameters** to display a work view.

d. On the work view, enter a domain name in the PC Domain Name field (1...15 alphanumeric characters).

e. On the toolbar, select Submit; then close work view.

f. Repeat for each domain of which this NE is a member.

21 ***NOTE:*** *Provisioning for TMN is now complete.*

Provision applications that use the TMN:

- TCP/IP Gateway (refer to Provisioning Guide)
- 1301 NMX Network Discovery [DLP-300]
- CDAC (refer to Provisioning Guide)
- RADMAP (refer to Provisioning Guide)
- Remote Logon [DLP-117]
- Serial E2A (refer to Provisioning Guide)

22 If the local NE is a Gateway NE to the X.25 Data Communications Network, provision the X.25 port and protocol stack (refer to Provisioning Guide).

23 STOP. This procedure is complete.

DLP-129
Provision Manual Area Address (MAADDR)

Purpose

This procedure describes how to provision the manual area address (MAADDR).

Prerequisites

Adhere to the following rules when provisioning the MAADDR on any NE in the network:

- If possible, place all NEs into a single area where each NE has only one MAADDR and the MAADDR is the same on all NEs. Use default values for MAADDR and ULSDCC provisioning so all NEs are level 1 Intermediate System (IS) NEs. (See Figure 1.)
- If multiple areas are required, each NE in an area should still have only one MAADDR entry, including the NEs provisioned for level 2 routing. Also NEs in the same area should have the same MAADDR entry.
- If areas are connected through level 2 IS NEs to create larger networks, MAADDRs on NEs in one area must be different than the MAADDRs on NEs in other areas.
- To collapse areas to create a single area, make sure that no more than three manual area addresses exist for all NEs in the newly created area. One way to achieve this is to go back to the NEs after the areas are collapsed and delete any unwanted MAADDR entries from the NEs.

General

There are several different ways to collapse areas. One way to collapse two areas that are linked using two level 2 IS NEs is to determine the MAADDR of an NE in one area and enter that same address on an NE in the other area.

If more than three MAADDR entries exist in a newly created area, some addresses may be dropped by the routing protocols and the user won't be aware of it. Depending on the addresses dropped (which follows an algorithm that is described in ISO 10589), some of the NEs in the network may be isolated from the network. Also, remote connections to and from these NEs may fail. To correct this situation, do the following:

1. Examine MAADDR provisioning on each NE in the area and determine how many different manual area addresses exist in the areas.
2. If there are more than three different addresses in the problem area, delete the excess MAADDRs.

After any MAADDR changes are made, allow 30 minutes for the changes to take effect and for the old information in the network to be eliminated.

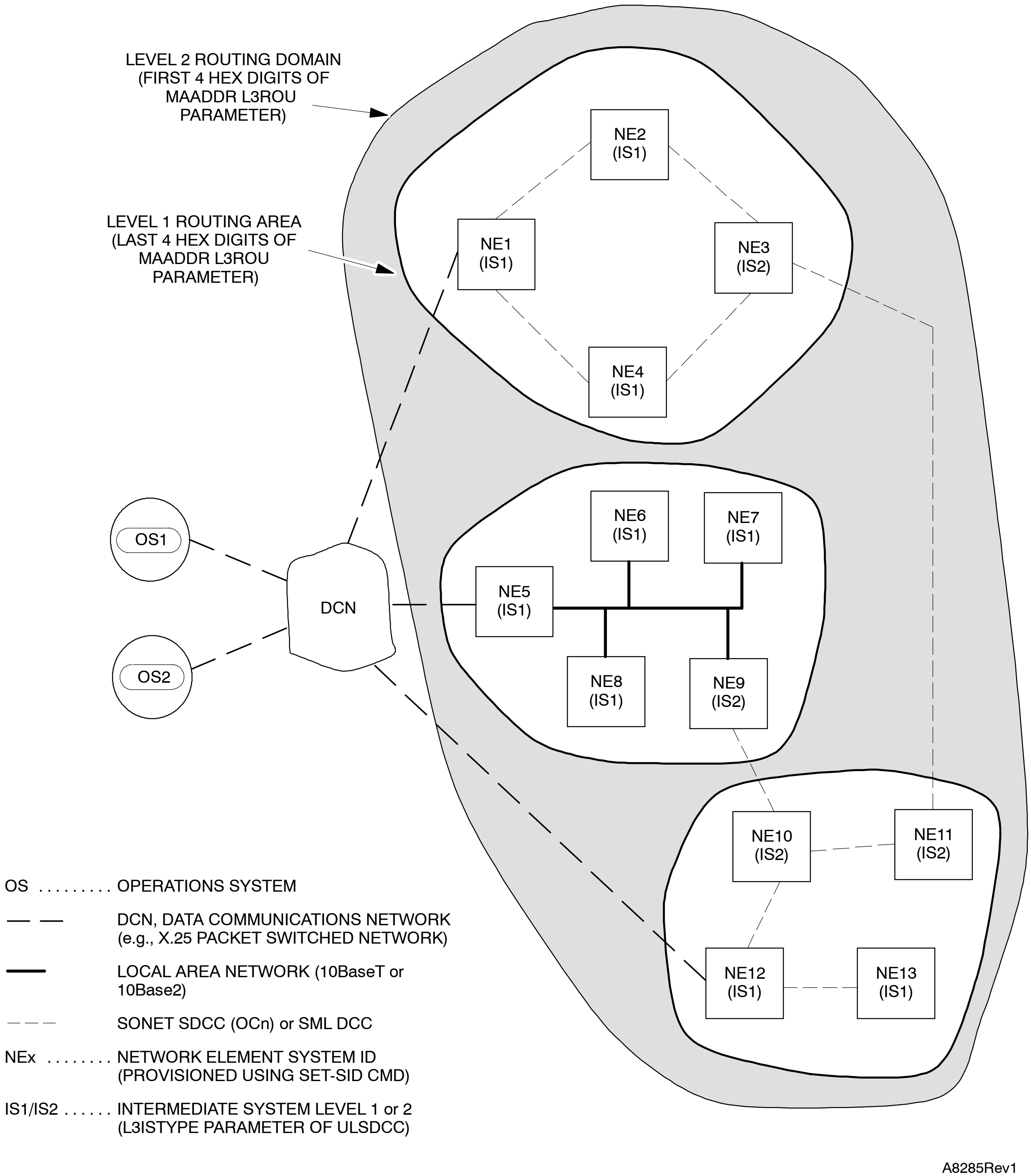
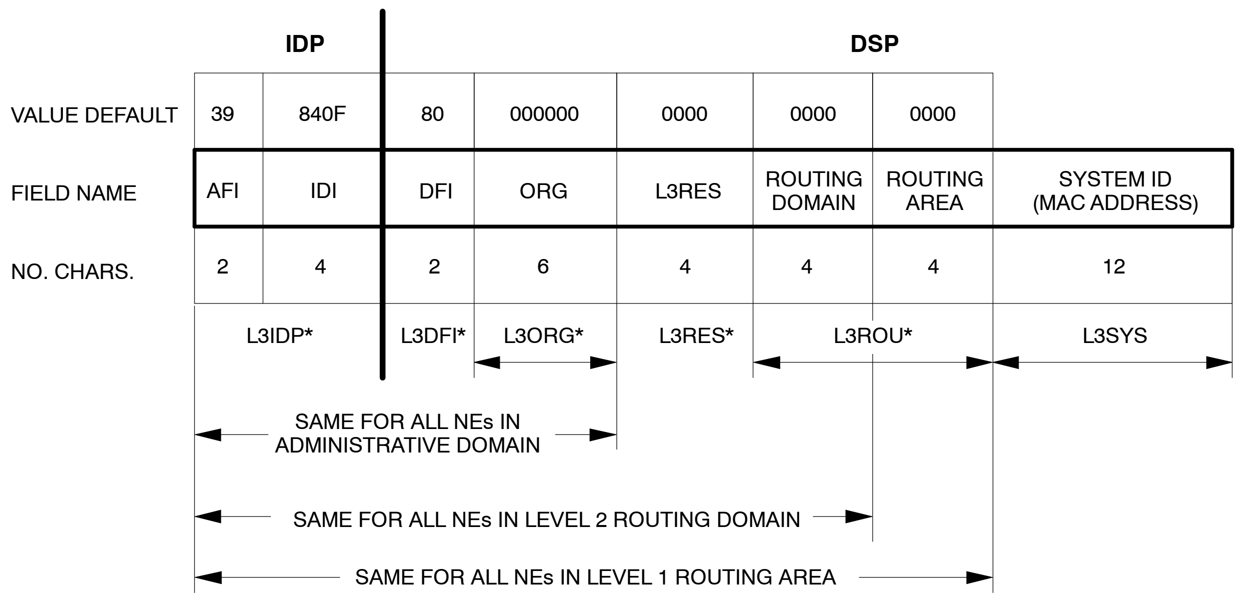


Figure 1. Example Telecommunications Management Network

STEP	PROCEDURE
1	**CAUTION: Possibility of service interruption. Changing the MAADDR alters the routing behavior of a network and can cause loss of communication between NEs. When changing the MAADDR of any NE in the network, follow the rules that appear in the Prerequisites and also review the information in the General section.**
2	See Figure 2 for a diagram of the Network Service Access Point (NSAP) address format.
3	In the scope pane, expand System; then expand General and select MAADDR.
4	In the result pane, right-click MAADDR being provisioned to display a context menu.
5	From the context menu, select **Provision Parameters** to display a work view.
6	From the Service State drop-down list, select In Service.
7	In Organization ID column, enter the Layer 3 Organization Identification part of the NSAP (six hexadecimal digits) for MAADDR ID 1.
8	In the Area Address column, enter the Layer 3 Routing and Area parts of the NSAP (eight hexadecimal digits – first four hexdigits are Level 2 Routing Domain and second four hexdigits are Level 1 Routing Area).
9	On the toolbar, select Submit; then close the work view (do not enter MAADDR ID 2 or 3).
10	STOP. This procedure is complete.



* THESE PARAMETERS ARE PROVISIONABLE (ALL OTHERS ARE FIXED)

IDP . . . . INITIAL DOMAIN PART OF THE NSAP

DSP . . . . DOMAIN SPECIFIC PART OF THE NSAP

AFI . . . . AUTHORITY AND FORMAT IDENTIFIER (FOR SONET, AFI IS 39 HEX TO IDENTIFY THE ISO-DCC ADDRESS FORMAT AND SYNTAX)

IDI . . . . INITIAL DOMAIN IDENTIFIER (IS 840 HEX IN THE UNITED STATES TO IDENTIFY THE NATIONAL BODY REPRESENTING THE USA IN ISO, WHICH IS ANSI). THE FOURTH CHARACTER POSITION OF THE IDI IS PADDED WITH AN “F”

DFI . . . . DSP FORMAT IDENTIFIER (IS 80 HEX TO IDENTIFY THIS FORMAT OF THE DSP)

ORG . . . . ORGANIZATION IDENTIFIER, IDENTIFIES THE ADMINISTRATIVE DOMAIN OF THE NETWORK PROVIDER (PROVISIONED WITH THE LSORG PARAMETER)

L3RES . . . . THIS FIELD IS RESERVED

ROUTING DOMAIN . . . . FIRST FOUR HEXADECIMAL CHARACTERS OF THE L3ROU PARAMETER THAT IDENTIFIES THE LEVEL 2 ROUTING DOMAIN

ROUTING AREA . . . . . . SECOND FOUR HEXADECIMAL CHARACTERS OF THE L3ROU PARAMETER THAT IDENTIFIES THE LEVEL 1 ROUTING AREA

SYSTEM ID . . . . INDIVIDUAL NE OR OS IDENTIFIER (UNIQUE VALUE STORED IN NONVOLATILE MEMORY ON THE COA PLUG-IN UNIT; IT IS RETRIEVED AS THE L3SYS PARAMETER BUT CANNOT BE CHANGED)

A8520Rev2

Figure 2. Network Service Access Point (NSAP) Format

DLP-300
Perform Network Discovery

Purpose

This procedure describes how to perform Network Discovery.

Prerequisites

Before starting this procedure, the following conditions should be met:

- Telecommunications Management Network (TMN) is established between all Network Elements (NEs) in network per DLP-128.
- Initial communication has been established with host NE per DLP-117.

General

Anytime there is a change in the network (NEs added, deleted, or moved from one PC domain to another), the network should be rediscovered and the PC domain lists updated and saved.

STEP	PROCEDURE
1	Retrieve alarms: a. In the scope pane, right-click NE name to display a context menu. b. From the context menu, select **Monitor Alarms** to display current alarms.
2	Are there any EOC alarms (LLSDCC, LLSMLDCC, LAN, etc.)? If yes, resolve alarms before continuing. If no, go to step 3.
3	If not already done, enter name of PC domain that this NE belongs to in the 1603 SMX NE database: a. In the scope pane, expand System; then expand Network Features and select PC Domains. b. In the result pane, right-click PC Domain being entered to display a context menu. c. From the context menu, select **Provision Parameters** to display a work view. d. On the work view, enter domain name in the PC Domain Name field (1...15 alphanumeric characters). e. On the toolbar, select Submit; then close work view.

4 Repeat step 3 for each domain of which this NE is a member.

5 Perform the following steps from the Explorer browser to discover the network:

a. In the Explorer browser scope pane, expand My Network and right-click on Network List.

b. From the context menu that is displayed, select **Create New NE List**.

c. Follow the instructions on each of the work views.

d. When you get to the last work view, select, Yes, create/update subnetworks; then select Finish. The newly discovered NEs are listed in the result pane.

6 STOP. This procedure is complete.

DLP-500
Run Equipment Diagnostics

Purpose

This procedure describes how to run diagnostics on a plug-in unit.

STEP	PROCEDURE
1	In the scope pane, expand Equipment and select the plug-in unit that you want to diagnose.
2	In the result pane, right-click unit being diagnosed to display a context menu.
3	From the context menu, select **Task>Operate>Diagnostics** to display a Diagnostic work view.
4	On the Diagnostic work view, select phase or phases that you want to run. **NOTE:** *To select more than one phase, hold down the Control key; then select the phases you want to run. To select all the phases, select the first phase, hold down the Shift key and select the last phase.*
5	In the Termination Method region, select Normal.
6	From Iterations spin-box, select number of times you want the diagnostic to run.
7	On the work view toolbar, select Submit icon.
8	Wait for diagnostics to complete (may take several minutes). **NOTE:** *While diagnostics are running, it is not possible to send other messages to the NE.* **NOTE:** *After the diagnostic tests complete, a PASS or FAIL appears for each phase in the Results column.*
9	Did diagnostics pass? If yes, go to step 12. If no, go to step 10.

10 On the work view toolbar, select the Information icon to display detailed information about the test (or tests) that failed.

11 After viewing the information, close the Details work view.

12 Close the Diagnostics work view.

13 STOP. This procedure is complete.

DLP-501
Retrieve/Change Service States

Purpose

This procedure describes how to retrieve and/or change the service state of an entity.

STEP	PROCEDURE
1	Find the entity for which you want to retrieve/change the service states in Table A.

Table A. Retrieving/Changing Service States

IF YOU WANT TO RETRIEVE/CHANE SERVICE STATES FOR...	THEN GO TO...
A plug-in unit (i.e., COA, HIF, LIF, etc.)	Step 2
A facility (i.e., OC3, OC12, EC1, etc.)	Step 10
A path (i.e., STS1, VT1.5, etc.)	Step 18
A protocol entity (i.e., LAN, X.25, TARP, etc.)	Step 27
A port (i.e., Craft 1, RS232, SML, etc.)	Step 35
A synchronization entity (i.e., NE Sync, BITS Sync, or BITS)	Step 50

Retrieve/Change Equipment Service State

2 In the scope pane, expand Equipment and select type of unit being checked.

3 In the result pane, find the plug-in unit you are checking in the Name column (e.g., DG2-LIF-A) and note the service state in the Primary State column.

4 Do you want to change the service state?

If yes, then continue to step 5.
If no, STOP. This procedure is complete.

5 In the result pane, right-click plug-in unit you want to change to display a context menu.

6 From the context menu, select **Provision Parameters** to open a Provision Parameters work view.

7 From the Service State drop-down list on the work view, select the new service state: In Service, Memory Administration, Maintenance, or Unassigned

NOTE: *If you are placing an Unassigned unit In Service, you need to select and equipment type (e.g., LIFD01) from the Equipment Type drop-down list.*

8 On the toolbar, select Submit icon; then close work view.

9 STOP. This procedure is complete.

Retrieve/Change Facility Service State

10 In the scope pane, expand Facility and select type of facility being checked.

11 In the result pane, find the facility you are checking in the Name column (e.g., DG3-OC12-1-A) and note the service state in the Primary State column.

12 Do you want to change the service state?

If yes, then continue to step 13.
If no, STOP. This procedure is complete.

13 In the result pane, right-click facility you want to change to display a context menu.

14 From the context menu, select **Provision Parameters** to display a Provision Parameters work view.

15 From the Service State drop-down list on the work view, select the new service state: In Service, Memory Administration, Maintenance, or Unassigned.

16 On the toolbar, select Submit icon; then close work view.

17 STOP. This procedure is complete.

Retrieve/Change Path Service State

18 In the scope pane, expand Facility; then expand facility type (i.e., OC3, EC1, etc.) that is carrying the path being checked.

19 Select path type that you are checking (i.e., STS1, VT1.5, etc.).

20 In the result pane, find the path you are checking in the Name column (e.g., DG2-STS1-5-A) and note the service state in the Primary state column.

21 Do you want to change the service state?

If yes, then continue to step 22.
If no, STOP. This procedure is complete.

22 In the result pane, right-click path you want to change to display a context menu.

23 From the context menu, select **Provision Parameters** to display a Provision Parameters work view.

24 From the Service State drop-down list on the work view, select either In Service or Memory Administration.

25 On the toolbar, select Submit icon; then close work view.

26 STOP. This procedure is complete.

Retrieve/Change Protocol Service State

27 In the scope pane, expand System; then expand Protocols and select the protocol you want to check (i.e., LAN, X.25, TARP, etc.).

28 In the result pane, note the service state of the entity in the Primary State column.

29 Do you want to change the service state?

If yes, then continue to step 30.
If no, STOP. This procedure is complete.

30 In the result pane, right-click a protocol name to display a context menu.

31 From the context menu, select **Provision Parameters** to display a Provision Parameters work view.

32 From the Service State drop-down list on the work view, select a new service state.

33 On the toolbar, select Submit icon; then close work view.

34 STOP. This procedure is complete.

Retrieve/Change Port Service State

35 Which port do you want to retrieve or change: Craft1, Craft 2, SE2A (serial E2A), X.25, PPP, or SML?

If Craft1, go to step 36.
If SML, go to step 39.
For all others, go to step 42.

36 In the scope pane, expand System; then expand Ports and select Craft-Front.

37 In the result pane, right-click Craft 1 to display a context menu.

38 Go to step 44.

39 In the scope pane, expand System; then expand Ports and select SML.

40 In the result pane, right-click SML to display a context menu.

41 Go to step 44.

42 In the scope pane, expand System; then expand Ports and select Craft-Rear.

43 In the result pane, right-click either Craft 2, PPP, SE2A, or X.25 Port to display a context menu.

44 From the context menu, select **Provision Parameters** to open a Provision Parameters work view.

45 On the work view, note the service state of the port (Service State column).

46 Do you want to change the service state?

If yes, then continue to step 47.
If no, STOP. This procedure is complete.

47 From the Service State drop-down list on the work view, select a new service state.

48 On the toolbar, select Submit icon; then close work view.

49 STOP. This procedure is complete.

Retrieve/Change Synchronization Service State (NE Sync, BITS, etc.)

50 In the scope pane, expand System; then expand Synchronization and select NE Sync, BITS Sync or BITS.

51 In the result pane, note the note the current service state in the Primary State column.

52 Do you want to change the service state?

If yes, then continue to step 53.
If no, STOP. This procedure is complete.

53 In the result pane, right-click NE Sync, BITS Sync, SYNCPRI, or SYNCSEC to display a context menu.

54 From the context menu, select **Provision Parameters** to display a Provision Parameters work view.

55 From the Service State drop-down list on the work view, select a new service state.

56 On the toolbar, select Submit icon; then close work view.

57 STOP. This procedure is complete.

DLP-502
Retrieve/Change Provisioned Parameters

Purpose

This procedure describes how to retrieve and/or change the provisioned parameters of an entity.

STEP	PROCEDURE

1 Find the entity on which you want to retrieve/change provisioned parameters in Table A.

Table A. Retrieving/Changing Provisioned Parameters

IF YOU WANT TO RETRIEVE/CHANGE PROVISIONED PARAMETERS...	THEN GO TO...
On BLSR ring	Step 2
On equipment (i.e., COA, HIF, LIF, etc.)	Step 11
On a facility (i.e., OC3, OC12, EC1, etc.)	Step 20
On a path (i.e., STS1, VT1.5, etc.)	Step 29
On a protocol entity (i.e., LAN, X.25, TARP, etc.)	Step 39
On a port (i.e., Craft 1, Craft 2, PPP, etc.)	Step 48
On a synchronization entity (i.e., NE Sync, BITS Sync, or BITS)	Step 64

Retrieve/Change Provisioned Parameters for BLSR Ring

2 In the scope pane, expand BLSR and select BLSR Ring.

3 In the result pane, right-click BLSR Ring to display a context menu.

4 From the context menu, select **Provision Parameters** to display a work view.

5 On the work view, note the provisioned values of the parameters.

6 Do you want to change any of the parameters?

If yes, then continue to step 7.
If no, then go to step 9.

7 On the work view, select a new setting from the drop-down list beside the parameter you want to change.

8 On the toolbar, select Submit icon.

9 Close work view.

10 STOP. This procedure is complete.

Retrieve/Change Provisioned Parameters for Equipment

11 In the scope pane, expand Equipment and select an equipment type, (i.e., HIF, LIF, DMI, CCM, etc.).

12 In the result pane, right-click unit you want to retrieve to display a context menu.

13 From the context menu, select **Provision Parameters** to display a Provision Parameters work view.

14 On the work view, note the provisioned values of the parameters.

15 Do you want to change any of the parameters?

If yes, then go to step 16.
If no, then go to step 18.

16 On the work view, select a new setting from the drop-down list below the parameter you want to change.

17 On the toolbar, select Submit icon.

18 Close work view.

19 STOP. This procedure is complete.

Retrieve/Change Provisioned Parameters for Facilities

20 In the scope pane, expand Facility and select type of facility being checked.

21 In the result pane, right-click facility you want to retrieve to display a context menu.

22 From the context menu, select **Provision Parameters** to display a Provision Parameters work view.

23 On the work view, note the provisioned values of the parameters.

24 Do you want to change any of the parameters?

If yes, then go to step 25.
If no, then go to step 27.

25 On the work view, select new a setting from the drop-down list below the parameter you want to change.

26 On the toolbar, select Submit icon; then close work view.

27 Close work view.

28 STOP. This procedure is complete.

Retrieve/Change Provisioned Parameters for Paths

29 In the scope pane, expand Facility; then expand facility type (i.e., OC3, EC1, etc.) that is carrying the path being checked.

30 Select path type that you are checking (i.e., STS1, VT1.5, etc.).

31 In the result pane, right-click path you want to retrieve to display a context menu.

32 From the context menu, select **Provision Parameters** to display a Provision Parameters work view.

33 On the work view, note the provisioned values of the parameters.

34 Do you want to change any of the parameters?

If yes, then go to step 35.
If no, then go to step 37.

35 On the work view, select a new setting from the drop-down list below the parameter you want to change.

36 On the toolbar, select Submit icon.

37 Close work view.

38 STOP. This procedure is complete.

Retrieve/Change Provisioned Parameters for Protocols

39 In the scope pane, expand System; then expand Protocols and select the protocol you want to retrieve (e.g., LAN, X.25, TARP, etc.).

40 In the result pane, right-click protocol you want to retrieve to display a context menu.

41 From the context menu, select **Provision Parameters** to display a Provision Parameters work view.

42 On the work view, note the provisioned values of the parameters.

43 Do you want to change any of the parameters?

If yes, then continue to step 44.
If no, then go to step 46.

44 On the work view, select a new setting from the drop-down list beside the parameter you want to change.

45 On the toolbar, select Submit icon.

46 Close Provision Parameters work view.

47 STOP. This procedure is complete.

Retrieve/Change Provisioned Parameters for Ports

48 Which port do you want to retrieve or change: Craft1, Craft 2, SE2A (serial E2A), X.25, PPP, or SML?

If Craft 1, go to step 49.
If SML, go to step 52.
For all others, go to step 55.

49 In the scope pane, expand System; then expand Ports and select Craft-Front.

50 In the result pane, right-click Craft 1 to display a context menu.

51 Go to step 57.

52 In the scope pane, expand System; then expand Ports and select SML.

53 In the result pane, right-click SML to display a context menu.

54 Go to step 57.

55 In the scope pane, expand System; then expand Ports and select Craft-Rear.

56 In the result pane, right-click either Craft 2, PPP, SE2A, or X.25 Port to display a context menu.

57 From the context menu, select **Provision Parameters** to display a Provision Parameters work view.

58 On the work view, note the provisioning for each of the parameters.

59 Do you want to change any of the parameters?

If yes, then continue to step 60.
If no, then go to step 62.

60 On the work view, select a new setting from the drop-down list under the parameter you want to change.

61 On the toolbar, select Submit icon.

62 Close Provision Parameters work view.

63 STOP. This procedure is complete.

Retrieve/Change Provisioned Parameters for Synchronization Entities

64 In the scope pane, expand System; then expand Synchronization and select NE Sync, BITS Sync or BITS.

65 In the result pane, right-click the sync entity you want to retrieve to display a context menu.

66 From the context menu, select **Provision Parameters** to display a Provision Parameters work view.

67 On the work view, note the provisioning for each of the parameters.

68 Do you want to change any of the parameters?

If yes, then continue to step 69.
If no, then go to step 71.

69 On the work view, select new settings from the drop-down list beside or under the sync parameter you want to change.

70 On the toolbar, select Submit icon.

71 Close the work view.

72 STOP. This procedure is complete.

DLP-503
Switch to an Alternate Sync Source/Release Sync Switch

Purpose

This procedure describes how to switch to an alternate synchronization source and how to release a sync switch.

STEP	PROCEDURE
1	In the scope pane, expand System; then expand Synchronization and select NE Sync or BITS Sync
2	In the result pane, right-click sync source you want to switch to.
3	From the context menu that is displayed, select **Task>Operate>Switch** to open an Operate Switch work view.
4	Do you want to switch to an alternate sync source and release the timing reference or just release the sync switch? If switch and release, then go to step 5. If just release, then go to step 7.
5	In the Switch To region of the work view, select the source you want to switch to.
6	On the toolbar, select Submit icon.
7	In the Switch To region, select Release radio button.
8	On the toolbar, select Submit again; then close work view.
9	STOP. This procedure is complete.

DLP-504
Retrieve, Create, Modify, or Delete a Cross-Connect

Purpose

This procedure describes how to retrieve, create, modify, or delete a cross-connect.

STEP	PROCEDURE
1	Find the task you want to perform in Table A.

Table A. Retrieve, Create, Modify, or Delete a Cross-Connect

IF YOU WANT TO...	THEN GO TO...
Retrieve a cross-connect	Step 2
Create a new cross-connect or re-establish an existing cross-connect	Step 8
Modify an existing cross-connect	Step 20
Delete an existing cross-connect	Step 29

Retrieve Cross-Connect

2 In the scope pane, expand Cross-Connect; then expand Connections and select type of path being retrieved (i.e., STS1, VT1.5, etc.).

3 In the result pane, right-click path being retrieved to display a context menu.

4 From the context menu, select **Provision** to display a Provision work view.

5 On the Provision work view, note cross-connect for selected path.

6 If you are not going to modify or delete the cross-connect, close work view.

7 STOP. This procedure is complete.

Create New Cross-Connect

8 In the scope pane, expand Cross-Connect; then select Connections.

9 Right-click in the result pane to display a context menu.

10 From the context menu, select **New** to display a New work view.

NOTE: *It takes several minutes for the New work view to be displayed.*

11 On New work view, select a connection type from the Connection Type drop-down list.

NOTE: *Diagrams of the possible connections for that connection type are displayed.*

12 From the Final Service State drop-down list on the work view, select either In Service or Memory Administration.

13 If several choices are for the selected Connection Type, select a connection diagram.

NOTE: *The cross-connection diagram you select appears in the Selected Diagram panel.*

14 Select a First Source, a Second Source (if necessary), and a Destination.

15 Select Add.

16 Close New work view and return to Provision work view.

17 On the Provision work view toolbar, select Submit icon.

18 Close work view.

19 STOP. This procedure is complete.

Modify Existing Cross-Connect

20 In the scope pane, expand Cross-Connect; then expand Connections and select type of path being modified (i.e., STS1, VT1.5, etc.).

21 In the result pane, right-click path being modified to display a context menu.

22 From the context menu, select **Provision** to display a Provision work view.

23 On the Provision work view toolbar, select the Modify icon to display a Modify work view.

24 On the Modify work view, select a connection type from the Connection Type drop-down list.

25 If applicable, select a second source from the Second Source drop-down list.

26 Select OK.

27 On the Provision work view toolbar, select Submit icon; then close work view.

28 STOP. This procedure is complete.

Delete Existing Cross-Connect

29 In the scope pane, expand Cross-Connect; then expand Connections and select the type of path for which you are deleting a cross-connect.

30 In the result pane, right-click cross-connect path being deleted to display a context menu.

31 From the context menu, select **Provision** to display a Provision work view.

32 On the Provision work view, select the cross-connect you want to delete.

33 On the Provision work view toolbar, select the Delete icon; then select the Submit icon.

34 Close the Provision work view.

35 STOP. This procedure is complete.

DLP-505
Switch to Redundant Unit

Purpose

This procedure describes how to switch the active and standby plug-in units.

STEP	PROCEDURE
1	In the scope pane, expand Equipment and select the type of plug-in unit (e.g., CLK, HIF, LIF, etc.) that you want to switch.
2	In the result pane, right-click name of unit you want to switch to display a context menu.
3	From the context menu that is displayed, select **Task>Operate>Switch** to open an Operate Switch work view.
4	In the Equipment region, select unit you want to switch.
5	In the Switch Mode region, select Manual radio button.
6	On the work view toolbar, select Submit icon.
7	Close the Operate Switch work view.
8	STOP. This procedure is complete.

DLP-506
Allow Automatic Switching to Redundant Unit

Purpose

This procedure describes how to allow automatic switching to redundant equipment for all redundant units as well as how to allow automatic switching for an individual unit.

STEP	PROCEDURE
1	Do you want to allow automatic switching for all redundant equipment or for an individual unit? If all, then continue to step 2. If individual, then go to step 10.

All Units

STEP	PROCEDURE
2	In the scope pane, expand System.
3	Expand General and select Global Settings.
4	In the result pane, right-click Global Settings to display a context menu.
5	From the context menu, select **Task>Provision>Allow/Inhibit** to display a Global Settings Provision Allow/Inhibit work view.
6	From the Sw to Dx drop-down list on the work view, select Allow.
7	On the work view toolbar, select Submit icon.
8	Close work view.
9	STOP. This procedure is complete.

Individual Unit

10 In the scope pane, expand Equipment and select the type of plug-in unit for which you want automatic switching to duplex allowed (e.g., CCM, DMI, LIF, etc.).

11 In the result pane, right-click unit being allowed to display a context menu.

12 From the context menu, select **Task>Provision>Allow/Inhibit** to display a Provision Allow/Inhibit work view.

13 From Sw to Dx drop-down list, select Allow.

14 On the work view toolbar, select Submit icon.

15 Close work view.

16 STOP. This procedure is complete.

DLP-507
Release Path Protection Switching

Purpose

This procedure describes how to release a path switch condition that inhibits automatic switching to a protection path.

STEP	PROCEDURE
1	In the scope pane, expand Facility.
2	Expand the facility type (i.e., OC3, EC1, DS3, etc.) that contains the path you want to release; then select the path type (i.e., STS1, VT1, etc.).
3	In the result pane, right-click alarmed path to display a context menu.
4	From the context menu, select **Task>Operate>Switch** to open a Path Switch work view.
5	Select active facility.
6	In the Switch Mode region, select Release radio button.
7	On the work view toolbar, select Submit icon.
8	Close work view.
9	STOP. This procedure is complete.

DLP-508
Delete TADRMap Pair

Purpose

This procedure describes how to delete a TADRMap pair.

STEP	PROCEDURE
1	In the scope pane, expand System.
2	Expand Protocols and select TADRMap.
3	In the result pane, right-click name of TADRMap pair that you want to delete.
4	From the context menu, select **Provision Parameters** to open a work view.
5	In the Name column on the work view, select the TADRMAP being deleted.
6	On the toolbar, select Delete icon; then select Submit icon.
7	Close work view.
8	STOP. This procedure is complete.

DLP-509
Retrieve/Change Expected Signal Label

Purpose

This procedure describes how to determine the provisioned value of the Expected Signal Label parameter and how to change this value.

STEP	PROCEDURE
1	In the scope pane, expand Facility.
2	Expand the facility that is carrying the alarmed path (i.e., OC3, EC1, etc.); then select the type of path (i.e., STS1, VT1.5, etc.) that is generating alarm.
3	In the result pane, right-click alarmed path to display a context menu.
4	From the context menu, select **Provision Parameters** to display a Provision Parameters work view.
5	On the Provision Parameters work view, note the provisioned value of the Expected Signal Label parameter.
6	Do you want to change the value of the Expected Signal Label parameter to agree with the incoming signal label? If yes, go to step 7. If no, go to step 9.
7	Use the spin box in the Expected Signal Label field to select a new value that matches the Incoming Signal Label.
8	On the work view toolbar, select Submit icon.
9	Close work view.
10	STOP. This procedure is complete.

DLP-510
Allow/Inhibit PM Reporting

Purpose

This procedure describes how to allow or inhibit PM reporting on entities.

STEP	PROCEDURE
1	Find the entity on which you want to allow/inhibit PM reporting in Table A.

Table A. Allow/Inhibit PM Reporting

IF YOU WANT TO...	THEN GO TO...
Allow/Inhibit PM reporting on all entities	Step 2
Allow/Inhibit PM reporting on AAL5	Step 8
Allow/Inhibit PM reporting on ATM Port	Step 14
Allow/Inhibit PM reporting on ATM Processor	Step 24
Allow/Inhibit PM reporting on facilities	Step 33
Allow/Inhibit PM reporting on POS Port	Step 39
Allow/Inhibit PM reporting on synchronization entities	Step 47
Allow/Inhibit PM reporting on equipment	Step 53
Allow/Inhibit PM reporting on STS or VT path	Step 59
Allow/Inhibit PM reporting on USRLAN facility	Step 66
Allow/Inhibit PM reporting on VCL	Step 74
Allow/Inhibit PM reporting on VPL	Step 84

Allow/Inhibit PM Reporting on All Entities

2 In the scope pane, expand System; then expand General and select Global Settings.

3 In the result pane, right-click Global Settings to display a context menu.

4 From the context menu that is displayed, select **Task>Provision>Allow/Inhibit** to open a Global Settings Provision Allow/Inhibit work view.

5 From the PM Report drop-down list on the work view, select Allow or Inhibit.

6 On the toolbar, select Submit icon; then close work view.

7 STOP. This procedure is complete.

Allow/Inhibit PM Reporting on AAL5

8 In the scope pane, expand Facility; then expand USRLAN and select AAL5.

9 In the result pane, right-click AID for AAL5 on which you want to allow PM reporting to display a context menu.

10 From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.

11 From QOS PM Report drop-down list on work view, select Allow or Inhibit.

12 On the toolbar, select Submit icon; then close work view.

13 STOP. This procedure is complete.

Allow/Inhibit PM Reporting on an ATM Port

14 In the scope pane, expand Facility; then expand USRLAN and select ATM Port.

15 In the result pane, right-click ATMPORT AID to display a context menu.

16 From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.

17 What type of PM reporting (NDC or QOS) do you want to allow or inhibit?

If NDC (Network Data Collection), then continue to step 18.
If QOS (Quality of Service), then go to step 21.

18 From NDC PM Report drop-down list on work view, select Allow or Inhibit.

19 On the toolbar, select Submit; then close work view.

20 STOP. This procedure is complete.

21 From QOS PM Report drop-down list on work view, select Allow or Inhibit.

22 On the toolbar, select Submit icon; then close work view.

23 STOP. This procedure is complete.

Allow/Inhibit PM Reporting for an ATM Processor

24 In the scope pane, expand Facility and select ATM Processor.

25 In the result pane, right-click ATMPROC AID to display a context menu.

26 From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.

27 What type of PM reporting (NDC, QOS, or NTM) do you want to allow or inhibit?

If NDC (Network Data Collection), then go to step 28.
If QOS (Quality of Service), then go to step 29.
If NTM (Network Traffic Management), then go to step 30

28 From NDC Report drop-down list on work view, select Allow or Inhibit; then go to step 31.

29 From QOS PM Report drop-down list on work view, select Allow or Inhibit; then go to step 31.

30 From NTM PM Report drop-down list on work view, select Allow or Inhibit; then go to step 31.

31 On the toolbar, select Submit icon; then close work view.

32 STOP. This procedure is complete.

Allow/Inhibit PM Reporting on a Facility

33 In the scope pane, expand Facility and select type of facility that has PM reporting inhibited.

34 In the result pane, right-click facility generating INHPMREPT alarm to display a context menu.

35 From the context menu, select **Task>Provision>Allow/Inhibit** to open a Provision Allow/Inhibit work view.

36 From the PM Report drop-down list on the work view, select Allow or Inhibit.

37 On the toolbar, select Submit icon; then close work view.

38 STOP. This procedure is complete.

Allow/Inhibit PM Reporting on POS Port

39 In the scope pane, expand URSLAN Facility and select POS Port.

40 In the result pane, right-click POS Port on which you want to allow or inhibit PM reporting.

41 From the context menu that is displayed, select **Task>Provision>Allow/Inhibit** to open a Provision Allow/Inhibit work view.

42 What type of PM reporting (NDC or QOS) do you want to allow or inhibit?

If NDC (Network Data Collection), then continue to step 43.
If QOS (Quality of Service), then go to step 44.

43 From NDC Report drop–down list on work view, select Allow or Inhibit; then go to step 45.

44 From the QOS PM or NDC PM Report drop-down list on the work view, select Allow or Inhibit.

45 On the toolbar, select Submit icon; then close work view.

46 STOP. This procedure is complete.

Allow/Inhibit PM Reporting of Synchronization Entity

47 In the scope pane, expand System; then expand Synchronization and select NE Sync or BITS Sync.

48 In the result pane, right-click Sync entity you want to allow or inhibit to display a context menu.

49 From the context menu, select **Task>Provision>Allow/Inhibit** to open a Provision Allow/Inhibit work view.

50 From the PM Report drop-down list on the work view, select Allow or Inhibit.

51 On the toolbar, select Submit icon; then close work view.

52 STOP. This procedure is complete.

Allow/Inhibit PM Reporting on Equipment

53 In the scope pane, expand Equipment and select type of unit on which you want to allow or inhibit PM reporting.

54 In the result pane, right-click unit type to display a context menu.

55 From the context menu, select **Task>Provision>Allow/Inhibit** to open a Provision Allow/Inhibit work view.

56 From the PM Report drop-down list on the work view, select Allow or Inhibit.

57 On the toolbar, select Submit icon; then close work view.

58 STOP. This procedure is complete.

Allow/Inhibit PM Reporting on an STS or VT Path

59 In the scope pane, expand Facility; then expand facility type that contains the alarmed path, (i.e., STS1, VT, etc.)

60 From the list of paths, select type of path that has PM reporting inhibited.

61 In the result pane, locate the path that is reporting the INHPMREPT alarm in the Name column and right-click on the path.

62 From the context menu that is displayed, select **Task>Provision>Allow/Inhibit** to open a work view.

63 From the PM Report drop-down list on the work view, select Allow or Inhibit.

64 On the toolbar, select Submit icon; then close work view.

65 STOP. This procedure is complete.

Allow/Inhibit PM Reporting on a USRLAN facility

66 In the scope pane, expand Facility and select USRLAN.

67 In the result pane, right-click USRLAN AID to display a context menu.

68 From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.

69 What type of PM reporting (NDC or QOS) do you want to allow or inhibit?

If NDC reports, then continue to step 70.
If QOS (Quality of Service), then go to step 71.

70 From NDC PM Report drop-down list on work view, select Allow or Inhibit; then go to step 72.

71 From QOS PM Report drop-down list on work view, select Allow or Inhibit.

72 On the toolbar, select Submit icon; then close work view.

73 STOP. This procedure is complete.

Allow/Inhibit PM Reporting on a VCL

74 In the scope pane, expand Facility; then expand USRLAN and select VCL.

75 In the result pane, right-click AID for VCL, on which you want to allow or inhibit PM reporting, to display a context menu.

76 From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.

77 What type of PM reporting (Connection QOS or Segment QOS) do you want to allow or inhibit?

If Connection QOS, then continue to step 78.
If Segment QOS, then go to step 81.

78 From Connection QOS PM Reports drop-down list on work view, select Allow or Inhibit.

79 On the toolbar, select Submit icon; then close work view.

80 STOP. This procedure is complete.

81 From Segment QOS PM Reports drop-down list on work view, select Allow or Inhibit.

82 On the toolbar, select Submit icon; then close work view.

83 STOP. This procedure is complete.

Allow/Inhibit PM Reporting on a VPL

84 In the scope pane, expand Facility; then expand USRLAN and select VPL.

85 In the result pane, right-click AID for VPL, on which you want to allow or inhibit PM reporting, to display a context menu.

86 From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.

87 What type of PM reporting (Connection QOS or Segment QOS) do you want to allow or inhibit?

If Connection QOS, then continue to step 88.
If Segment QOS, then go to step 91.

88 From Connection QOS PM Reports drop-down list on work view, select Allow or Inhibit.

89 On the toolbar, select Submit icon; then close work view.

90 STOP. This procedure is complete.

91 From Segment QOS PM Reports drop-down list on work view, select Allow or Inhibit.

92 On the toolbar, select Submit icon; then close work view.

93 STOP. This procedure is complete.

DLP-511
Determine/Change Payload Type

Purpose

This procedure describes how to determine the type of payload a path is carrying. It also describes how to change the type of payload.

STEP	PROCEDURE
1	In the scope pane, expand Facility.
2	Expand facility type (i.e., OC3, DS3, EC1, etc.) that contains the alarmed path.
3	Select type of path (i.e., STS1, STS3c, etc.) that is carrying the payload.
4	In the result pane, find the path in the Name column and note payload in Payload Type column.
5	Do you want to change the payload type? If yes, then continue to step 6. If no, then go to step 11.
6	In the result pane, right-click path that you want to change in Name column.
7	From the context menu that is displayed, select **Provision Payload Type** to display a Provision Payload Type work view.
8	From the Payload Type drop-down list on the work view, select VT or STS.
9	On the toolbar, select Submit icon.
10	Close work view.
11	STOP. This procedure is complete.

DLP-512
Retrieve/Change Expected Incoming Path Trace

Purpose

This procedure describes how to retrieve and change the incoming path trace.

STEP	PROCEDURE
1	In the scope pane, expand Facility.
2	Expand facility type (i.e., OC3, EC1, etc.) that contains the path; then select the path type (i.e., STS1, STS3c, or STS12c).
3	In the result pane, right-click the path being retrieved or changed to display a context menu.
4	From the context menu, select the **Task>Provision>Path Trace** to open a Provision Path Trace work view.
5	Do you want to change the path trace? If yes, then continue to step 6. If no, then go to step 8
6	Enter a new value in the Expected Incoming field.
7	On the toolbar, select Submit.
8	Close work view.
9	STOP. This procedure is complete.

DLP-513
Switch Service Away from Alarmed Facility

Purpose

This procedure describes how to switch service away from an alarmed facility.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select alarmed OC facility.
2	In the result pane, right-click facility being switched to display context menu.
3	From the context menu, select **Task>Operate>Switch** to open an Operate Switch APS work view.
4	On the work view, select active facility.
5	In the Switch Mode region, select Forced radio button.
6	On the toolbar, select Submit.
7	Close work view.
8	STOP. This procedure is complete.

DLP-514
Retrieve/Change Outgoing Path Trace

Purpose

This procedure describes how to determine the outgoing path trace and if necessary how to change it.

STEP	PROCEDURE
1	In the scope pane, expand Facility.
2	Expand facility type (i.e., OC3, EC1, etc.) that contains the path; then select the path type (i.e., STS1, STS3c, or STS12c).
3	In the result pane, right-click the path being retrieved or changed to display a context menu.
4	From the context menu, select the **Task>Provision>Path Trace** to open a Provision Path Trace work view.
5	In the Provisioned Outgoing column on the work view, note the value of the outgoing path trace.
6	Do you want to change the provisioned value? If yes, then continue to step 7. If no, then go to step 9.
7	Enter a new value in the Provisioned Outgoing field.
8	On the toolbar, select Submit.
9	Close work view.
10	STOP. This procedure is complete.

DLP-515
Switch OCn Facility

Purpose

This procedure describes how to switch an OCn facility to test protection switching.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select OC3, OC12, or OC48.
2	In the result pane, right-click OCn facility being switched to display a context menu.
3	From the context menu, select **Task>Operate>Switch** to open a work view.
4	On work view, select active OCn facility.
5	In the Switch Mode region, select Manual radio button.
6	On the toolbar, select Submit icon.
7	Wait for switch to take place; then close work view.
8	STOP. This procedure is complete.

DLP-516
Retrieve/Change Enhanced Remote Defect Indicator (ERDI) Parameter

Purpose

This procedure describes how to retrieve the ERDI parameter and how to change the provisioned value.

STEP	PROCEDURE
1	In the scope pane, expand Facility.
2	Expand facility type (i.e., OC3, EC1, DS3, etc.) carrying alarmed path; then select path type (i.e., STS1, VT1.5, etc.).
3	In the result pane, right-click alarmed path to display a context menu.
4	From the context menu, select **Provision Parameters** to display a path Provision Parameters work view.
5	On the work view, note the setting for the Enhanced Remote Defect Indicator parameter.
6	Do you want to change the parameter? If yes, go to step 7. If no, then go to step 9.
7	From the Enhanced Remote Defect Indicator drop-down list on the work view, select either Yes or No.
8	On the toolbar, select Submit icon.
9	Close work view.
10	STOP. This procedure is complete.

DLP-517
Retrieve PM Register Contents

Purpose

This procedure describes how to determine the contents of a Performance Monitor (PM) register.

STEP	PROCEDURE

1 Refer to Table A for selections to make in the scope pane.

Table A. Scope Pane Selections for Retrieving PM Registers

TO RETRIEVE PM REGISTER CONTENTS FOR...	IN SCOPE PANE EXPAND...	THEN EXPAND...	AND SELECT...
Equipment	Equipment	–	LIF, LDR, DMI, VTG, CCM, or CLK
Facilities	Facility	–	OC3, OC12, OC48, EC1, DS3, DS3/DS1 Tmux, or DS1
Paths	Facility	Facility Type	STS1, STS3c, STS12c, VCL, or VPL
USRLAN Facility, AAL5, ATM Port, VCL, VPL, or POS Port	Facility	USRLAN	Entity being retrieved (i.e., AAL5, POS Port, etc.)
ATM Processor	Facility	–	ATM Processor
NE Sync	System	Synchronization	NE Sync

2 In the result pane, right-click entity for which you are retrieving PM register contents.

3 From the context menu that is displayed, select **Task>Monitor>Performance** to open a Monitor Performance work view.

4 In the Name column on the work view, locate the PM you are checking and note the contents of the register.

5 Close the work view.

6 STOP. This procedure is complete.

DLP-518
Handling Static-Sensitive Devices

Purpose

This procedure describes how to handle static-sensitive devices.

STEP	PROCEDURE
1	***WARNING: Possibility of damage to equipment. Plug-in units contain static-sensitive devices. These devices are susceptible to static discharge damage in unconnected circuit conditions. The following procedure should always be followed when installing or removing the plug-in units.***
2	Wear a grounded wrist strap.
3	Connect ground wrist straps to grounding jacks located to the right of the Power Distribution Units.
4	Handle units at front and side edges only. Do not touch circuit traces or components.
5	STOP. This procedure is complete.

DLP-519
Retrieve/Change DS3 Format Parameter

Purpose

This procedure describes how to retrieve the provisioned value for the DS3 Format parameter and if necessary how to change the parameter.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select DS3. **NOTE:** *If T3 is connected to an LIF601, expand DS3/DS1 TransMux after expanding Facility; then select DS3.*
2	In the result pane, right-click DS3 facility reporting alarm to display a context menu.
3	From the context menu, select **Provision Parameters** to display a Provision Parameters work view.
4	On the work view, note provisioned value of DS3 Format parameter.
5	Do you want to change DS3 Format parameter? If yes, go to step 6. If no, then go to step 8.
6	From DS3 Format drop-down list, select a new format value.
7	On the toolbar, select Submit icon.
8	Close work view.
9	STOP. This procedure is complete.

DLP-520
Retrieve/Change Security Provisioning

Purpose

This procedure describes how to retrieve/change security provisioning.

STEP	PROCEDURE

1 Find the type of privilege codes you want to retrieve or change in Table A.

Table A. Retrieving/Changing Security Provisioning

IF YOU WANT TO...	THEN GO TO...
Retrieve/change user privilege codes	Step 2
Retrieve/change command privilege codes	Step 22
Retrieve/change channel (port) privilege codes	Step 12
Retrieve/change password privilege codes	Step 32

Retrieve/Change User Privilege Codes

2 In the scope pane, expand System; then expand Security and select User.

3 In the result pane, locate the user's name and note the privilege code levels assigned to that user for Maintenance, Provisioning, Security, and Test.

4 Do the user privilege codes need to be changed?

NOTE: *Changes to the user privilege codes must be made by the system administrator.*

If yes, go to step 5.
If no, go to step 10.

5 In the result pane, right-click the name of the user whose privilege codes are being changed.

6 From the context menu that is displayed, select **Provision** to open a work view.

7 On the work view, find the user's name in the Name column; then move the cursor to the Privilege Code columns on that row and select the privilege code level you want to change.

NOTE: *A spin box appears when the privilege code is selected.*

8 Use the spin box to change the privilege code.

9 On the toolbar, select Submit icon; then close the work view.

10 Close work view.

11 STOP. This procedure is complete.

Retrieve/Change Channel Privilege Codes

12 In the scope pane, expand System; then expand Security and select Channel.

13 In the result pane, locate the Access Type and note the privilege code levels assigned for Maintenance, Provisioning, Security, and Test.

14 Do you want to make any changes?

NOTE: *Changes must be made by the system administrator.*

If yes, go to step 15.
If no, go to step 20.

15 In the result pane, right-click Access Type being changed to display a context menu.

16 From the context menu, select **Provision** to open a work view.

17 On the work view, move the cursor to the Privilege Code columns and select the privilege code that you want to change.

NOTE: *A spin box appears when the value or privilege code is selected.*

18 Use the spin box to change the value or privilege code.

19 On the toolbar, select Submit icon.

20 Close the work view.

21 STOP. This procedure is complete.

Retrieve/Change Command Privilege Codes

22 In the scope pane, expand System; then expand Security and select Command.

23 In the result pane, right-click Command Privileges to display a context menu.

24 From the context menu, select **Provision** to open a work view.

25 On the work view, note the levels of Maintenance, Provisioning, Security, and Test privilege codes for the command of interest.

26 Do any of the command privilege codes need to be changed?

NOTE: *Changes to the command privilege codes must be made by the system administrator.*

If yes, go to step 27.
If no, go to step 30.

27 Find the command name in the Command ID column; then move the cursor to the Privilege columns on that row and select the privilege code you want to change.

NOTE: *A spin box appears when the privilege code is selected.*

28 Use the spin box to change the privilege code.

29 On the toolbar, select Submit icon.

30 Close the work view.

31 STOP. This procedure is complete.

Retrieve/Change Password Privilege Codes

32 In the scope pane, expand System; then expand Security and select Password.

33 In the result pane, right-click Modify Password to display a context menu.

34 From the context menu, select **Modify Password** to open a Modify Password work view.

35 On the work view, enter the User ID and the old password; then enter a new password and verify it.

36 On the toolbar, select Submit icon.

37 Close the work view.

38 STOP. This procedure is complete.

DLP-521
Check Version of Software/Firmware Installed on a Unit

Purpose

This procedure describes how to determine the version of software (and if applicable, firmware) that is installed on a plug-in unit.

STEP	PROCEDURE
1	In the scope pane, expand System and select Inventory.
2	In the result pane, right-click Software Inventory to display a context menu.
3	From the context menu, select **View** to open a Software Inventory work view.
4	In the Unit column on the work view, locate the unit you are checking. To the right of that unit, locate the Software Revision column and note the version of software installed on that unit. ***NOTE:*** *If the NE contains an LIF901 unit, the Embedded Firmware Version and Inuse Firmware are also included on the work view.*
5	Close work view.
6	STOP. This procedure is complete.

DLP-522
Allow Diagnostics

Purpose

This procedure describes how to allow diagnostics on an individual entity or on all entities.

STEP	PROCEDURE
1	Do you want to allow diagnostics on an individual entity or on all entities? If all, then continue to step 2. If individual, then go to step 9.

All Units

STEP	PROCEDURE
2	In the scope pane, expand System; then expand General and select Global Settings.
3	In the result pane, right-click Global Settings to display a context menu.
4	From the context menu, select **Task>Provision>Allow/Inhibit** to open a Global Settings Provision Allow/Inhibit work view.
5	From the Diagnostics drop-down list on the work view, select Allow.
6	On the work view toolbar, select Submit icon.
7	Close work view.
8	STOP. This procedure is complete.

Individual Unit

STEP	PROCEDURE
9	In the scope pane, expand Equipment and select the type of plug-in unit that has had diagnostics inhibited (e.g., CCM, DMI, LIF, etc.).
10	In the result pane, right-click unit on which you want to allow diagnostics.
11	From the context menu that is displayed, select **Task>Provision>Allow/Inhibit** to display a Provision Allow/Inhibit work view.

12 From the Diagnostics drop-down list on the work view, select Allow.

13 On the work view toolbar, select Submit icon.

14 Close the work view.

15 STOP. This procedure is complete.

DLP-523
Release Loopback Tests

Purpose

This procedure describes how to release loopback tests that have been established.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select the type of facility (i.e., OC3, EC1, DS3, etc.) that has a loopback established.
2	In the result pane, right-click facility on which tests are to be released to display a context menu.
3	From the context menu, select **Task>Operate>Loopbacks** to display an Operate Loopbacks work view.
4	From the Loop Mode drop-down list, select Clear.
5	On the toolbar, select Submit.
6	Close work view.
7	STOP. This procedure is complete.

DLP-524
Retrieve/Change DS1 Frame Format and Line Code Parameters

Purpose

This procedure describes how to retrieve and (if necessary) change the DS1 Frame Format and Line Code parameters.

STEP	PROCEDURE
1	In the scope pane, expand Facility; then expand DS3/DS1 TransMux and select DS1.
2	In the result pane, right-click DS1 facility to display a context menu.
3	From the context menu, select **Provision Parameters** to open a work view.
4	On the work view, note how DS1 Format and Line Code parameters are provisioned.
5	Do you want to change DS1 Format or Line Code parameter? If DS1 Format parameter, then go to step 6. If Line Code parameter, then go to step 7. If no, then go to step 9.
6	From the DS1 Format drop-down list on the work view, select Clear Channel, Extended Super Frame, or Super Frame; then go to step 8.
7	From the Line Code drop-down list on the work view, select AMI or B8ZS; then go to step 8.
8	On the toolbar, select Submit icon.
9	Close work view.
10	STOP. This procedure is complete.

DLP-525
Retrieve/Change Provisioning of Line Buildout Parameter

Purpose

This procedure describes how to determine the provisioned value of the Line Buildout parameter and how to change that value.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select the type of facility (i.e., DS3 or EC1) that is generating the alarm.
2	In the result pane, right-click facility generating alarm to display a context menu.
3	From the context menu, select **Provision Parameters** to display a Provision Parameters work view.
4	On the work view, note how the Line Buildout parameter is provisioned.
5	Do you want to change the provisioned value? If yes, go to step 6. If no, go to step 8.
6	On the Line Buildout drop-down list, select Yes or No.
7	On the toolbar, select Submit icon.
8	Close work view.
9	STOP. This procedure is complete.

DLP-526
Determine Download Status of NE

Purpose

This procedure describes how to check the progress of a software download.

STEP	PROCEDURE
1	In the scope pane, right click NE name (e.g., Raleigh 1603 SMX) to display a context menu.
2	From the context menu, select **Task>Download>Download Status** to display a Download Status work view.
3	On the work view, note the status of the download.
4	Close the work view.
5	STOP. This procedure is complete.

DLP-527
Allow Automatic Download

Purpose

This procedure describes how to enable the auto-download feature.

STEP	PROCEDURE
1	In the scope pane, expand System; then expand General and select Global Settings.
2	In the result pane, right-click on Global Settings to display a context menu.
3	From the context menu, select **Provision Parameters-NE** to open a work view.
4	From the Auto Download Feature drop-down list on the work view, select Allow.
5	On the toolbar, select Submit icon.
6	Close the work view.
7	STOP. This procedure is complete.

DLP-528
Retrieve/Initialize Logs

Purpose

This procedure describes how to retrieve or initialize the following logs: alarm/event messages log and security log.

STEP	PROCEDURE

1 Find the type of log you want to retrieve in Table A.

Table A. Retrieving/Initializing Logs

IF YOU WANT TO...	THEN GO TO...
Retrieve the alarm/event messages log	Step 2
Initialize the alarm/event messages log	Step 8
Retrieve the security log	Step 13
Initialize the security log	Step 18

Retrieve Alarm/Event Messages Log

2 In the scope pane, expand System and select Logs.

3 In the result pane, right-click Alarm/Event Messages Log to display a context menu.

4 From the context menu, select **View** to display the Alarm/Event Messages Log work view.

5 Locate the alarm you are trying to clear in the Conditions column and note any entries in the Details column.

6 Close work view.

7 STOP. This procedure is complete.

Initialize Alarm/Event Messages Log

8 In the scope pane, expand System and select Logs.

9 In the result pane, right-click Alarm/Event Messages Log to display a context menu.

10 From the context menu, select **Clear Log**.

11 ***NOTE:*** *An Error dialog appears to warn you that you are about to clear all entries in the Log and asks if you want to continue.*

Select Yes button.

12 STOP. This procedure is complete.

Retrieve Security Log

13 In the scope pane, expand System and select Logs.

14 In the result pane, right-click Security Log to display a context menu.

15 From the context menu, select **View** to display the security log.

16 Note entries in the log; then close work view.

17 STOP. This procedure is complete.

Initialize Security Log

18 In the scope pane, expand System and select Logs.

19 In the result pane, right-click Security Log to display a context menu.

20 From the context menu, select **Clear Log**.

21 ***NOTE:*** *An Error dialog appears to warn you that you are about to clear all entries in the Log and asks if you want to continue.*

Select Yes button.

22 STOP. This procedure is complete.

DLP-529
Switch a Working Unit to Protection

Purpose

This procedure describes how switch a working LDR501 or VTG to a protection unit.

STEP	PROCEDURE
	NOTE: *Revertive switch may occur. Inhibit switch back to working if required.*
1	In the scope pane, expand Equipment and select type of unit to be switched (i.e., LDR or VTG).
2	In the result pane, right-click the working LDR501 or VTG being switched (e.g., DG3-GRP1-LDR-1) to display a context menu.
3	From the context menu, select **Task>Operate>Switch** to open an Operate Switch work view.
4	In Equipment region, select working unit being switched to protection (e.g., DG3-GRP1-LDR-1).
5	In the Switch Mode region, select Manual radio button.
6	On the work view toolbar, select Submit icon. **NOTE:** *Service condition of working unit changes to standby and protection unit changes to active.*
7	Close work view.
8	STOP. This procedure is complete.

DLP-530
Change Traffic Descriptor Characteristics

Purpose

This procedure describes how to change the traffic descriptor characteristics.

General

A traffic descriptor is a mechanism used to provide a traffic management function on an ATM VP connection. On a 1603 SMX, a traffic descriptor can be created for each ATM service offering on an Ethernet interface (LIF901). An example of an ATM service would be Constant Bit Rate (CBR) and Variable Bit Rate (VBR) service categories at an n x 1 Mbit Ethernet bandwidth.

Each NE supports 32 unique traffic descriptors that are used with each individual Ethernet ATM VP. The same traffic descriptor can be used for many VPs. Refer to Table A for a description of the parameters provisioned with each traffic descriptor.

Table A. Traffic Descriptor Provisioning

FIELD	DESCRIPTION	ALLOWED VALUES
Name	User name associated with traffic descriptor	1...32 Noncase-sensitive Alphanumeric characters
Profile Type	Profile indication	PT1, PT2, PT3, PT4, PT5, PT6*
Peak Cell Rate for CLP 0 and CLP 1 Cells (PCR0 +1)	Peak cell rate of all cells (CLP=0 and 1) in cells per second	100...353,207
Sustained Cell Rate for CLP 0 and CLP 1 Cells (SCR0+1)	Sustained cell rate of all cells (CLP=0 and 1) in cells per second	100...353,207
Maximum Burst Size for CLP 0 and CLP 1 Cells (MBS0+1)	Maximum burst size of all cells (CLP=0 and 1) in number of cells	32, 50, 100, 150, 210
* *PT1, PT2, PT3, and PT4 are for future applications.*		

STEP	PROCEDURE
1	Determine name of traffic descriptor that you want to change: a. In the scope pane, expand Facility; then expand USRLAN and select AAL5. b. In the result pane, select AAL5 to display a context menu. c. From the context menu, select Provision Parameters to open a work view. d. In the Ingress Traffic Descriptor Name column, note name of traffic descriptor that you want to change. e. Close work view.
2	Retrieve Traffic Descriptor Provision Parameters work view: a. In the scope pane, expand System; then expand Network Features and select Traffic Descriptor. b. In the result pane, select the traffic descriptor identified in step 1 to display a context menu. c. From the context menu, select Provision Parameters to open the Traffic Descriptor Provision Parameters work view.
3	On the work view, select the traffic descriptor that you want to change. **NOTE:** *Steps 4 through 7 provide assistance in selecting values for the parameters found on the Traffic Descriptors Provision Parameters work view.*
4	If you want to change the profile type, make a selection from the Profile Type drop-down list. (Refer to Table B.) **NOTE:** *An Ethernet ATM interface uses traffic descriptors with profile types 5 or 6. Profile type 5 is used for constant bit rate services and profile type 6 is used for variable bit rate services. Profile types 1 - 4 are for future applications.*

Table B. Profile Types

PROFILE TYPE	PCR0	PCR0+1	CDVT	SCR0	SCR0+1	MBS0	MBS0+1	GCRA
1	–	X	X	–	–	–	–	1
2	–	X	X	–	X	–	X	2
3	–	X	X	X	–	X	–	2
4	X	X	X	–	–	–	–	2
Profile Types for ATM Cell Sources (used on LIF901)								
5	–	X	–	–	–	–	–	1
6	–	X	–	–	X	–	X	2

5 To change Peak Cell Rate (PCR) for CLP 0 or CLP 1 Cells, select a different value in spin box. (Refer to Table C for information on setting peak cell rates.)

NOTE: *For an Ethernet ATM interface, the peak cell rate should not exceed the capacity of the link exiting the Ethernet ATM interface toward an ATM router.*

6 To change Sustained Cell Rate (SCR) for CLP 0 or CLP 1 Cells, select a different value in spin box. (Refer to Table C for information on setting sustained cell rate values.)

NOTE: *The SCR parameter is associated with Variable Bit Rate (VBR) service categories. SCR is not used by Constant Bit Rate (CBR) service categories. The sustained cell rate must always be less than the peak cell rate.*

7 To change Maximum Burst Size for CLP 0 or CLP 1 Cells, select a different value from drop-down list. (Refer to Table D for maximum burst size values supported by the 1603 SMX.)

NOTE: *The Maximum Burst Size (MBS) parameter is associated with variable bit rate (VBR) service categories. MBS is not used by constant bit rate (CBR) service categories. Appropriate values for the maximum burst size parameter depend on both the network and the service offering. The maximum burst size should be set to a value that allows one or more complete information units (i.e., packets, PDUs, etc.) to enter or transit the ATM network at the peak cell rate without causing degradation in overall network performance. You must select a maximum burst size for an Ethernet ATM interface.*

8 After traffic descriptor changes have been made, select Submit; then close work view.

9 STOP. This procedure is complete.

Table C. ATM Peak and Sustained Cell Rates*

APPLICATION	PCR OR SCR VALUE (CELLS/SEC)	TOTAL OR AVERAGE ATM CELL BANDWIDTH (BITS/SEC)	USER CELLS (CELLS/SEC)	OAM CELLS (CELLS/SEC)	MAXIMUM OR MAXIMUM AVERAGE USER PAYLOAD (BITS/SEC)
ATM Mapped Links					
56 kbit Link	133	56,000	131	2	50,304
n x 56 kbit Link	n x 133	n x 56,000	n x 131	n x 2	n x 50,304
DS0 Link	152	64,000	150	2	57,600
n x DS0 Link	n x 152	n x 64,000	n x 150	n x 2	n x 57,600
STS-1 Link	114,113	48,384,000	113,219	894	43,476,176
STS-3c Link	353,207	149,760,000	350,467	2,740	134,579,000
Services Through ATM					
10 Mbit Ethernet Maximum Median	26,623	11,288,000	26,416	207	11,200,338
10 Mbit Ethernet Maximum Average	26,905	11,408,000	26,695	209	11,319,067
10 Mbit Ethernet Maximum	34,673	14,701,000	34,404	269	14,587,200
100 Mbit Ethernet Maximum Median	266,229	112,880,000	264,159	2,070	112,003,381
100 Mbit Ethernet Maximum Average	269,049	114,080,000	266,959	2,090	113,190,666
100 Mbit Ethernet Maximum	346,727	147,010,000	344,037	2,690	145,872,000
n x 1 Mbit Ethernet Average	n x 2627	n x 1,113,424	n x 2605	n x 22	n x 1,000,320

Table C. ATM Peak and Sustained Cell Rates*

APPLICATION	PCR OR SCR VALUE (CELLS/SEC)	TOTAL OR AVERAGE ATM CELL BANDWIDTH (BITS/SEC)	USER CELLS (CELLS/SEC)	OAM CELLS (CELLS/SEC)	MAXIMUM OR MAXIMUM AVERAGE USER PAYLOAD (BITS/SEC)
n x 1 Mbit Ethernet Average link utilization	n x 2358	n x 1,000,000	n x 2338	n x 20	n x 987,792

* *The top portion of this table lists peak cell rates for various ATM links used to transport ATM cells. The bottom portion of the table lists peak cell rates for various ATM services or subscriptions. When using data from this table, keep in mind that an ATM link can carry more than one ATM service. For 1603 SMX, an ATM service is associated with each individual VP.*

Table D. Maximum Burst Size (MBS) Values

MAXIMUM BURST SIZE	SERVICE INFORMATION UNIT
32 Cells	Maximum length Ethernet packet (1518 Byte)
50 Cells	
100 Cells	
150 Cells	
210 Cells	Maximum length Subscriber Interface Protocol (SIP) Level 3 Protocol Data Unit (L3_PDU)

DLP-531
Retrieve/Change Equalization Distance Parameter

Purpose

This procedure describes how to retrieve and change the equalization distance parameter on an SML port or a BITS entity.

STEP	PROCEDURE
1	Do you want to retrieve/change the equalization distance parameter on an SML Port or on a BITS entity? If SML Port, go to step 2. If BITS entity, then go to step 12.

Retrieve/Change Equalization Distance Parameter on SML Port

STEP	PROCEDURE
2	In the scope pane, expand System; then expand Ports and select SML.
3	In the result pane, right-click SML to display a context menu.
4	From the context menu, select **Provision Parameters** to open a Provision Parameters work view.
5	On the work view, note the setting of the Equalization Distance parameter.
6	Do you want to change the parameter setting? If yes, go to step 7. If no, go to step 10.
7	Select the current setting for the Equalization Distance parameter. ***NOTE:*** *A spin box appears when the parameter setting is selected.*
8	Use the spin box to change the setting.
9	On the toolbar, select the Submit icon.
10	Close the work view.
11	STOP. This procedure is complete.

Retrieve/Change Equalization Distance Parameter on BITS

12 In the scope pane, expand System; then expand Synchronization and select BITS.

13 In the result pane, right-click SYNCPRI or SYNCSEC to display a context menu.

14 From the context menu, select **Provision Parameters** to open a Provision Parameters work view.

15 On the work view, note the setting of the Equalization Distance parameter.

16 Do you want to change the parameter setting?

If yes, go to step 17.
If no, go to step 20.

17 Select the current setting for the Equalization Distance parameter.

NOTE: *A spin box appears when the parameter setting is selected.*

18 Use the spin box to change the setting.

19 On the toolbar, select the Submit icon.

20 Close the work view.

21 STOP. This procedure is complete.

DLP-532
Allow Automatic Download of Firmware

Purpose

It is possible to inhibit automatic downloading of firmware to an LIF901 unit. This procedure describes how to remove that inhibit.

STEP	PROCEDURE
1	In the scope pane, expand System.
2	Expand General and select Global Settings.
3	In the result pane, right-click Global Settings to display a context menu.
4	From the context menu, select **Provision Parameters-NE** to open a work view.
5	In NE Allow/Inhibit region of work view, select Allow from Auto Download ATM LAN drop-down list.
6	On the toolbar, select Submit icon.
7	Close work view.
8	STOP. This procedure is complete.

DLP-533
Manually Download Firmware

Purpose

This procedure describes how to manually download firmware to an LIF901 unit.

STEP	PROCEDURE
1	In the scope pane, right-click NE name to display a context menu.
2	From the context menu, select **Task>Download>Copy Program Local** to open a Copy Program Local work view.
3	In the Copy To: region on the work view, select DGx-LIF-A-FW in the Unit column.
4	In the Copy From: region on the work view, select Auto Select.
5	On the toolbar, select Submit icon. ***NOTE:*** *During the download process, LEDs on the front panel of the LIF901 light in a scrolling pattern.*
6	After download completes, close work view.
7	STOP. This procedure is complete.

DLP-534
Change Alarm Notification Code

Purpose

This procedure describes how to change an alarm notification code for common NE alarms and plug-in unit alarms.

STEP	PROCEDURE
1	Do you want to change an alarm notification code for common NE alarms or for a plug-in unit? If common NE alarms, then go to step 2. If plug-in unit alarms, then go to step 9.

Change Notification Code for Common NE Alarms

2	In the scope pane, select Common.
3	In the result pane, right-click COM to display a context menu.
4	From the context menu, select **Provision Alarm Conditions** to display a Provision Alarm Conditions work view.
5	From Condition drop-down list, select alarm to change (e.g., PROGVER).
6	From Active or A Side Notification Code drop-down list, select a notification code (i.e., Minor Alarm, Not Alarmed, Not Reported, etc.).
7	On the toolbar, select Submit icon; then close work view.
8	STOP. This procedure is complete.

Change Notification Code for Plug−in Unit Alarms

9	In the scope pane, expand Equipment and select a plug-in unit.
10	In the result pane, right-click unit that you want to change to display a context menu.

11 From the context menu, select **Task>Provision>Alarm Conditions** to display a Provision Alarm Conditions work view.

12 From Condition drop-down list, select alarm to change (e.g., FWMNVER).

13 From Active or A Side Notification Code drop-down list, select a notification code (i.e., Minor Alarm, Not Alarmed, Not Reported, etc.).

14 On the toolbar, select Submit icon; then close work view.

15 STOP. This procedure is complete.

DLP-535
Allow Switching to Protection Unit

Purpose

Not all units have 1:1 protection. In some instances, several working (active) units are backed up by a single unit. This backup unit is referred to as a protection unit. The capability exists to inhibit a working unit from switching to a protection unit. This procedure describes how to remove that inhibit from an individual unit or from all units that are backed up by a protection unit.

STEP	PROCEDURE
1	Find the type of switching you want to allow in Table A.

Table A. Switching to a Protection Unit

IF YOU WANT TO...	THEN GO TO...
Allow switching to all protection units	Step 2
Only allow switching on a specific unit	Step 9

All Protection Units

2	In the scope pane, expand System.
3	Expand General and select Global Settings.
4	In the result pane, right-click Global Settings to display a context menu.
5	From the context menu, select **Task>Provision>Allow/Inhibit** to display a Global Settings Provision Allow/Inhibit work view.
6	From the Sw to Prot drop-down list on the work view, select Allow.
7	On the toolbar, select Submit icon; then close work view.
8	STOP. This procedure is complete.

Specific Unit

9 In the scope pane, expand Equipment and select LDR or VTG.

10 In the result pane, right-click unit that you want to allow to switch. A context menu is displayed.

11 From the context menu, select **Task>Provision>Allow/Inhibit** to display a Provision Allow/Inhibit work view.

12 From the Sw to Prot drop-down list, select Allow.

13 On the toolbar, select Submit icon.

14 Close work view.

15 STOP. This procedure is complete.

DLP-536
Allow Switching to Working Unit

Purpose

For those equipment types that are supported by 1:3 or 1:7 protection, the capability exists to inhibit a protection unit from switching back to working after a fault is cleared. This procedure describes how to remove an inhibit from all units that are supported by this type of protection or from an individual unit.

STEP	PROCEDURE

1 Find the type of switching you want to allow in Table A.

Table A. Switching to a Working Unit

IF YOU WANT TO...	THEN GO TO...
Globally allow switching back to a working unit	Step 2
Only allow switching on a specific unit	Step 9

Globally Allow Switching

2 In the scope pane, expand System.

3 Expand General and select Global Settings.

4 In the result pane, right-click Global Settings to display a context menu.

5 From the context menu, select **Task>Provision>Allow/Inhibit** to display a Global Settings Provision Allow/Inhibit work view.

6 From the Sw to Wkg drop-down list on the work view, select Allow.

7 On the toolbar, select Submit icon; then close work view.

8 STOP. This procedure is complete.

Specific Unit

9 In the scope pane, expand Equipment and select LDR or VTG.

10 In the result pane, right-click alarmed unit to display a context menu.

11 From the context menu, select **Task>Provision>Allow/Inhibit** to display a Provision Allow/Inhibit work view.

12 From the Sw to Wkg drop-down list on the work view, select Allow.

13 On the toolbar, select Submit icon; then close work view.

14 STOP. This procedure is complete.

DLP-537
Retrieve Hardware/Software Inventory

Purpose

This procedure describes how to retrieve the hardware and/or software inventory for the 1603 SMX.

STEP	PROCEDURE
1	In the scope pane, expand System and select Inventory.
2	Do you want to retrieve hardware or software inventory? If hardware, then go to step 3. If software, then go to step 7.
3	In the result pane, right-click Hardware Inventory to display a context menu.
4	From the context menu, select **View** to display a Hardware Inventory work view.
5	After noting the hardware types, close work view.
6	STOP. This procedure is complete.
7	In the result pane, right-click Software Inventory to display a context menu.
8	From the context menu, select **View** to display a Software Inventory work view.
9	After noting the software releases, close work view.
10	STOP. This procedure is complete.

DLP-538
Copy Provisioning Database To/From COA or NEP

Purpose

This procedure describes how to copy the provisioning database from the NEP to the COA or from the COA to the NEP.

STEP	PROCEDURE
1	**CAUTION: Possibility of service interruption. The provisioning database may be overwritten if the wrong menu selections are made in this procedure.**
2	Is provisioning database being copied from NEP to COA (i.e., Working to Primary) or COA to NEP (i.e., Primary to Working)? If NEP to COA, then go to step 3. If COA to NEP, then go to step 5.
3	Copy database from NEP to COA (Working to Primary): a. In the scope pane, right-click NE name to display a context menu. b. From the context menu, select **Task>Copy Database** to open a work view. c. From the work view, select Working to Primary radio button. d. On the toolbar, select Submit; then close work view.
4	STOP. This procedure is complete.
5	Copy database from COA to NEP (Primary to Working): a. In the scope pane, right-click NE name to display a context menu. b. From the context menu, select **Task>Copy Database** to open a work view. c. From the work view, select Primary to Working radio button. d. On the toolbar, select Submit; then close work view. ***NOTE:*** *Do not enter any other commands until the copy completes.*
6	STOP. This procedure is complete.

DLP-539
Retrieve/Change BITS Frame Format and Line Code Parameters

Purpose

This procedure describes how to retrieve (and change if necessary) the BITS Frame Format and Line Code parameters.

STEP	PROCEDURE
1	In the scope pane, expand System; then expand Synchronization and select BITS.
2	In the result pane, right-click SYNCPRI or SYNCSEC to display a context menu.
3	From the context menu, select **Provision Parameters** to open a work view.
4	On the work view, note how Format Format and Line Code parameters are provisioned.
5	Do you want to change Frame Format or Line Code parameter? If Frame Format parameter, then go to step 6. If Line Code parameter, then go to step 7. If no, then go to step 9.
6	From the Frame Format drop-down list, select Extended Super Frame or Super Frame; then go to step 8.
7	From the Line Code drop-down list, select AMI or B8ZS.
8	On the toolbar, select Submit icon.
9	Close work view.
10	STOP. This procedure is complete.

DLP-540
Restart Laser

Purpose

This procedure describes how to restart the laser after it has automatically shutdown.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select the type of facility on which laser has shutdown (i.e., OC48, OC12, or OC3).
2	In the result pane, right-click facility with the shutdown laser to display a context menu.
3	From the context menu, select **Task>Operate>Laser Shutdown Override** to display an Operate Laser Shutdown Override work view.
4	From the list of facility names on the work view, select the facility on which you want to restart the laser.
5	In the Mode region, select Manual radio button.
6	On the toolbar, select Submit icon.
7	Close work view.
8	STOP. This procedure is complete.

DLP-541
Retrieve/Change Provisioning of Protection Switching Parameters

Purpose

This procedure describes how to retrieve the provisioned values for the Protection Switching parameters and how to change these values.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select type of OC facility.
2	In the result pane, right-click alarmed OC facility to display a context menu.
3	From the context menu, select **Task>Provision>Switch** to display a Provision Switch work view.
4	On the work view, note how the Protection Switching parameters (Switching Direction and Switching Mode) are provisioned.
5	Do you want to change either of the Protection Switching parameters? If yes, then go to step 6. If no, then go to step 11.
6	Do you want to change the Switching Direction or Switching Mode parameter. If Switching Direction, then go to step 7. If Switching Mode, then go to step 8.
7	From the drop-down list in the Switching Direction column, select either Unidirectional or Bidirectional; then go to step 10.
8	From the drop-down list in the Switching Mode column, select either Revertive or Non-Revertive.
9	If you selected Revertive switch mode, select the delay time using the spin box under the Delay Before Reverting parameter.
10	On the toolbar, select Submit icon; then close work view.
11	STOP. This procedure is complete.

DLP-542
Create a New Entry in BLSR Manual Sequence Map

Purpose

This procedure describes how to create a new entry in the manual sequence map.

STEP	PROCEDURE
1	In the scope pane, expand BLSR; then expand Sequence Map and select Manual Map.
2	Are there any entries in the result pane? If yes, then go to 5. If no, then go to 3.
3	Right-click anywhere in the result pane to display a context menu.
4	From the context menu, select New to open a work view; then go to step 7.
5	In the result pane, right-click a map entry to display a context menu.
6	From the context menu, select **Provision Parameters** to open a work view.
7	On the work view toolbar, select the New icon to add a new row to the work view.
8	In the new row, left-click in the Ring Node ID column to display a spin box.
9	Using the spin box, select a Node ID that is not used by any other node on the ring.
10	In the new row, left-click in the LG1 Neighbor Node ID column to display a spin box.
11	Using the spin box, select the Node ID of the LG1 NE neighbor.
12	In the new row, left-click in the LG2 Neighbor Node ID column to display a spin box.
13	On the toolbar, select Submit icon; then close work view.
14	STOP. This procedure is complete.

DLP-543
Retrieve/Change BLSR Ring Parameters

Purpose

This procedure describes how to retrieve BLSR ring parameters such as Node Identifier, BLSR Mode, etc. and how to change these parameters.

STEP	PROCEDURE
1	In the scope pane, expand BLSR and select BLSR Ring.
2	In the result pane, note status of parameters for NE of interest.
3	Do you want to change parameters for any of the NEs? If yes, then continue to step 4. If no, STOP. This procedure is complete.
4	In result pane, right-click BLSR Ring to open a context menu.
5	From context menu, select **Provision Parameters** to open a BLSR Ring Provision Parameters work view.
6	In the Global Settings region, use the drop-down list or spin box beside each parameter to select a new value. ***NOTE:*** *To change the Node Identifier, you need to select Unlock from the Node ID Unlock drop-down list.*
7	On the toolbar, select Submit icon; then close work view.
8	STOP. This procedure is complete.

DLP-544
Allow Automatic BLSR Ring Switch Exercise

Purpose

This procedure describes how to remove the inhibit that prevents an automatically scheduled BLSR switching exercise from running.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select OC48.
2	In the result pane, right-click OC48 facility(ies) on which you want to allow the switching exercise (e.g., LG1-OC48-A).
3	From the context menu that is displayed, select **Task>Provision>Allow/Inhibit** to open a Provision Allow/Inhibit work view.
4	From BLSR Switching Exercise drop-down list on the work view, select Allow.
5	On the toolbar, select Submit icon.
6	Close work view.
7	STOP. This procedure is complete.

DLP-545
Release (Allow) Forced/Locked-Out Facility Switch

Purpose

This procedure describes how to release a forced switch or a locked-out switch condition and allow facility switching to take place.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select OC3, OC12, or OC48.
2	In the result pane, right-click facility being released to display a context menu.
3	From the context menu, select **Task>Operate>Switch>APS** or **Task>Operate>Switch>BLSR** to open a work view.
4	On the work view, select active facility.
5	In the Switch Mode region, select Release radio button.
6	On the toolbar, select Submit icon.
7	Wait for progress bar to reach completion; then close work view.
8	STOP. This procedure is complete.

DLP-546
Disable Monitoring of Section Trace

Purpose

This procedure describes how to disable monitoring of a section trace.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select type of facility that contains the section trace.
2	In the result pane, right-click the facility that contains the section trace to display a context menu.
3	From the context menu, select **Task>Provision>Section Trace** to open a Provision Section Trace work view.
4	From Trace Format drop-down list on the work view, select ID.
5	On the toolbar, select Submit icon.
6	Close work view.
7	STOP. This procedure is complete.

DLP-547
Retrieve/Change Section Trace Data

Purpose

This procedure describes how to retrieve and change section trace data.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select type of facility generating the alarm (i.e., OC3, OC12, EC1, etc.)
2	In the result pane, right-click name of facility generating the alarm to display a context menu.
3	From the context menu, select **Task>Provision>Section Trace** to open a work view.
4	On the work view, note section trace data.
5	Do you want to change provisioned section trace values (i.e., provisioned outgoing or expected incoming)? If yes, then go to step 6. If no, then go to step 9.
6	***NOTE:*** *The Trace Format field must be TR1 (Provisionable Format) before the section trace values can be changed.* From the Trace Format drop-down list, select TR1.
7	Use the spin box under Provisioned Outgoing or Expected Incoming to change the provisioned value.
8	On the toolbar, select Submit icon.
9	Close work view.
10	STOP. This procedure is complete.

DLP-548
Allow Remote Activation of Loopbacks

Purpose

This procedure describes how to allow the remote activation of loopbacks.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select type of facility being allowed.
2	In the result pane, right-click facility being allowed to display a context menu.
3	From the context menu, select **Task>Provision>Allow/Inhibit** to open a work view.
4	From Loopback drop-down list, select Allow.
5	On the toolbar, select Submit icon.
6	Close work view.
7	STOP. This procedure is complete.

DLP-549
Add New COA to Database

Purpose

This procedure describes how to add a new COA to the database.

STEP	PROCEDURE
1	In the scope pane, expand Equipment and select COA.
2	In the result pane, right-click COA to display a context menu.
3	From the context menu, select **Provision Parameters** to open a Provision Parameters work view.
4	From the Equipment Type drop-down list, select equipment type of new unit (i.e., COA605, COA608, etc.).
5	From the Compatibility Code drop-down list, select a compatibility code.
6	On the toolbar, select the Submit icon.
7	Close work view.
8	STOP. This procedure is complete.

DLP-550
Retrieve NSAPs

Purpose

This procedure describes how to retrieve the Network Service Access Point (NSAP) of the local NE and NSAPs of direct neighbors.

STEP	PROCEDURE
1	Which NSAP(s) do you want to retrieve? If local, then go to step 2. If direct neighbor, then go to step 7.
2	In the scope pane, expand System; then expand Network Features and select NSAP.
3	In the result pane, right-click Local NSAP to display a context menu.
4	From the context menu, select **View** to open a work view. ***NOTE:*** *The work view identifies the link, NE name, and NSAP of the local NE.*
5	Close the work view.
6	STOP. This procedure is complete.
7	In the scope pane, expand System; then expand Network Features and select NSAP.
8	In the result pane, right-click Direct Neighbors to display a context menu.
9	From the context menu, select **View** to open a work view. ***NOTE:*** *The work view identifies the link, NE name, and NSAPs of the NEs direct neighbors.*
10	Close the work view.
11	STOP. This procedure is complete.

DLP-551
Retrieve/Change Provisioned Lower Layer DCC Data

Purpose

This procedure describes how to retrieve and modify the lower layer DCC parameters.

STEP	PROCEDURE
1	In the scope pane, expand System; then expand Ports and select SML.
2	In the result pane, right-click SML Port to display a context menu.
3	From the context menu, select **Task>Provision>DCC-Lower Layer** to open an SML Provision DCC-Lower Layer work view.
4	On the work view, note service state and provisioning of Side Role for the SML.
5	Do you want to change the provisioning of either of these parameters? If yes, go to step 6. If no, go to step 8.
6	Use the drop-down list under the parameter to change the value.
7	On the toolbar, select Submit icon.
8	Close work view.
9	STOP. This procedure is complete.

DLP-552
Retrieve/Change Provisioned Data for NE Environmental Alarms and Controls

Purpose

This procedure describes how to retrieve (and if necessary change) NE environmental alarms and controls.

STEP	PROCEDURE
1	Do you want to retrieve/change environmental alarms or environmental controls? If environmental alarms, go to step 2. If environmental controls, go to step 10.

Retrieve/Change Environmental Alarms

STEP	PROCEDURE
2	In the scope pane, expand System; then expand Network Features and select Env Alarms.
3	In the result pane, right-click ENV-n to display a context menu.
4	From the context menu, select **Provision Alarms** to display a Provision Alarms work view.
5	Note the provisioned data for the environmental alarm.
6	Do you want to change any of the provisioned data? If yes, go to step 7. If no, STOP. This procedure is complete.
7	To change Alarm Name or Destination NE, enter a new value in the parameter field. To change the other parameters, select a new setting from the drop-down list below the parameter.
8	On the toolbar, select Submit icon; then close work view.
9	STOP. This procedure is complete.

Retrieve/Change Environmental Controls

10 In the scope pane, expand System; then expand Network Features and select Env Controls.

11 In the result pane, right-click CONT-n to display a context menu.

12 From the context menu, select **Provision Controls** to display an Env Controls Provision Controls work view.

13 Note the provisioned data for the environmental controls.

14 Do you want to change any of the provisioned data?

If yes, go to step 15.
If no, STOP. This procedure is complete.

15 To change Control Name or Source NE, enter a new value in the parameter field. To change Source Type or Source Alarm ID, select a new setting from the drop-down list below the parameter.

16 On the toolbar, select Submit icon; then close work view.

17 STOP. This procedure is complete.

DLP-553
Verify Orderwire, Serial E2A TBOS and Craft 2 Port Wiring

Purpose

This procedure verifies the orderwire, serial E2A TBOS (Telemetry Byte-Oriented Serial), and Craft 2 port wiring.

STEP	PROCEDURE
1	See Figure 1 for shelf backplane locations referred to in this procedure.
2	Is orderwire interface provided? If yes, go to step 3. If no, go to step 7.
3	**NOTE:** *The OW1 wire-wrap pins are for LOCAL orderwire connections; the OW2 wire-wrap pins are for EXPRESS orderwire connections.* See Figures 2 and 3. Locate orderwire wire-wrap pins on shelf backplane and central office orderwire unit.
4	Verify that shielded cables (two 26 AWG pairs per orderwire interface) are properly terminated between shelf and orderwire unit.
5	Verify tip and ring integrity. Verify that cable shields terminate on frame ground (FG) pins on backplane.
6	**NOTE:** *The COA60x supports both an RS-232 and RS-422 interface. The RS-232 interface is used for connecting to a modem, video terminal or Personal Computer (PC). The PC may be used for running Serial E2A TBOS applications. The RS-422 interface is used for connecting to TBOS Alarm Processing Remote (APR) office subsystems.* **NOTE:** *The RS-232 interface requires an odd-numbered COA unit (COA601, 603, etc.). The RS-422 interface requires an even-numbered COA unit (COA602, 604, etc.).* Is Craft 2 port wiring provided? If no, STOP. This procedure is complete. If yes and it's RS-232, go to step 7. If yes and it's RS-422 (TBOS), go to step 15.

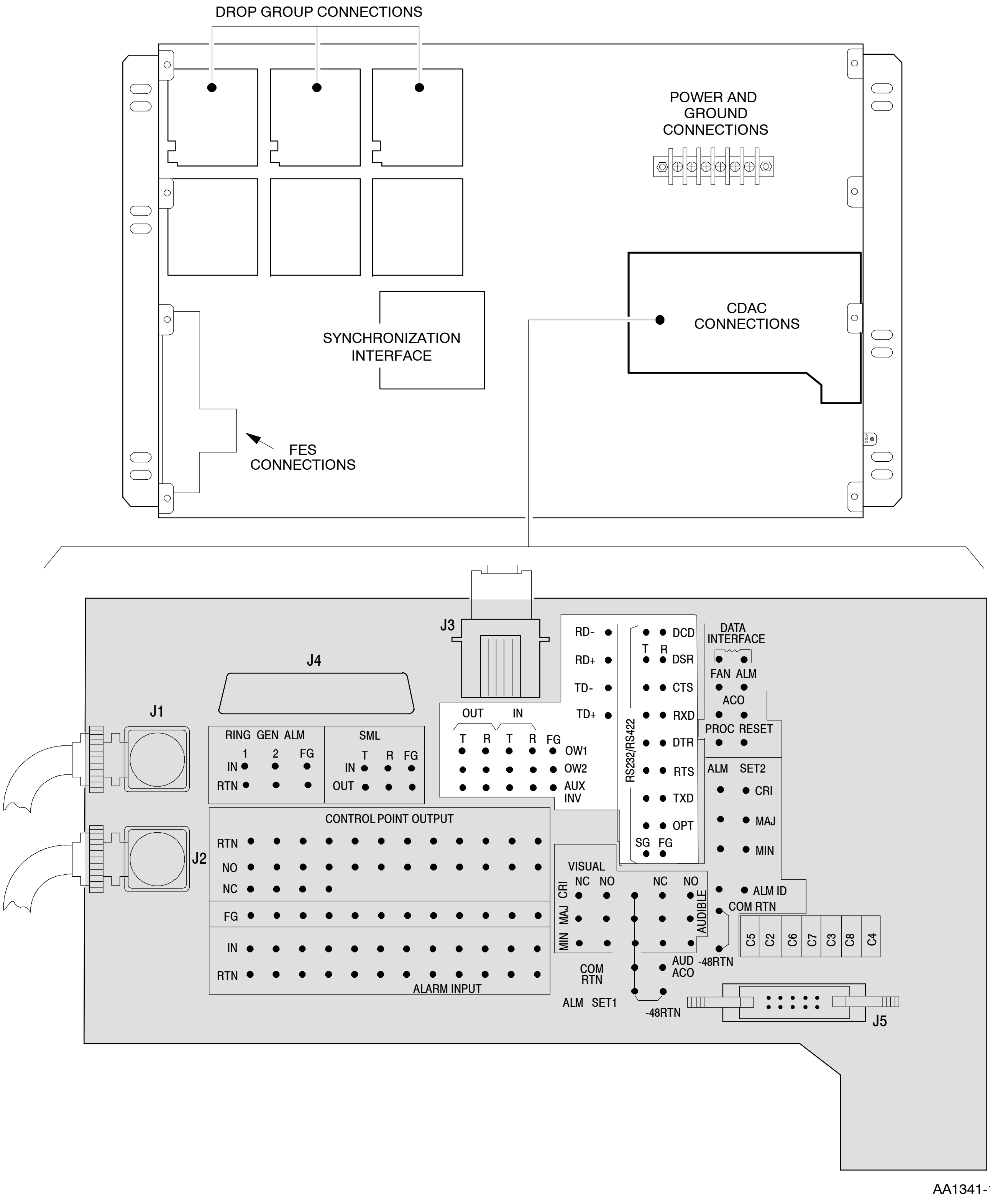


Figure 1. 1603 SMX Rear View

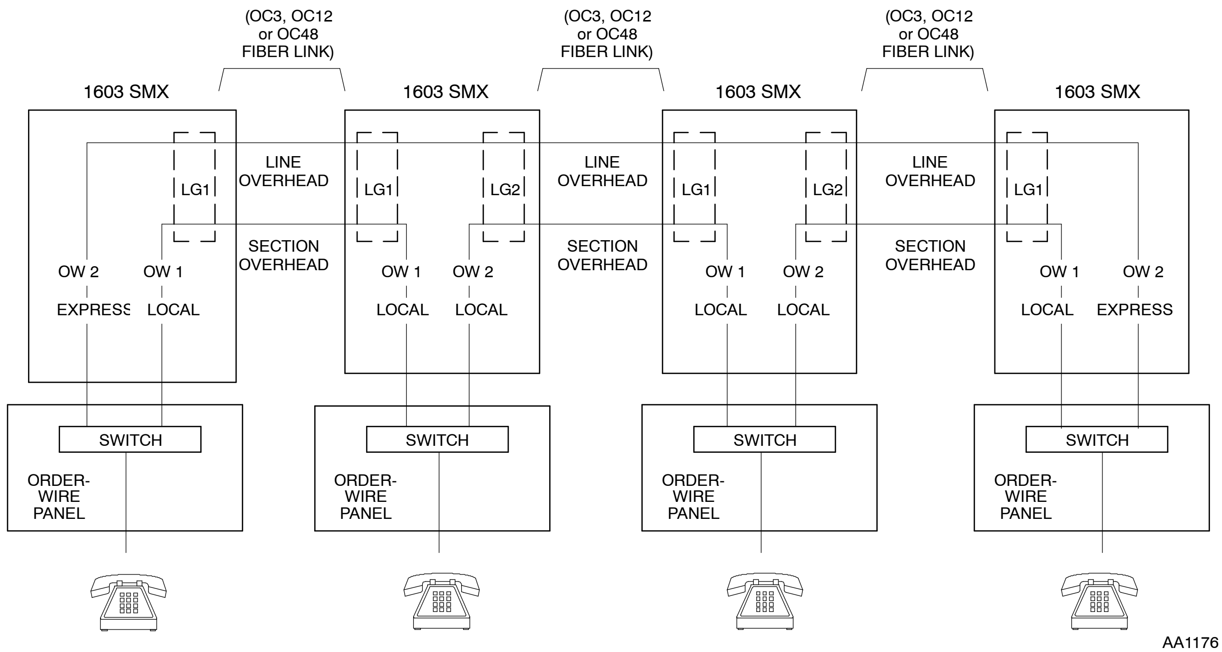


Figure 2. Orderwire Analog Interfaces

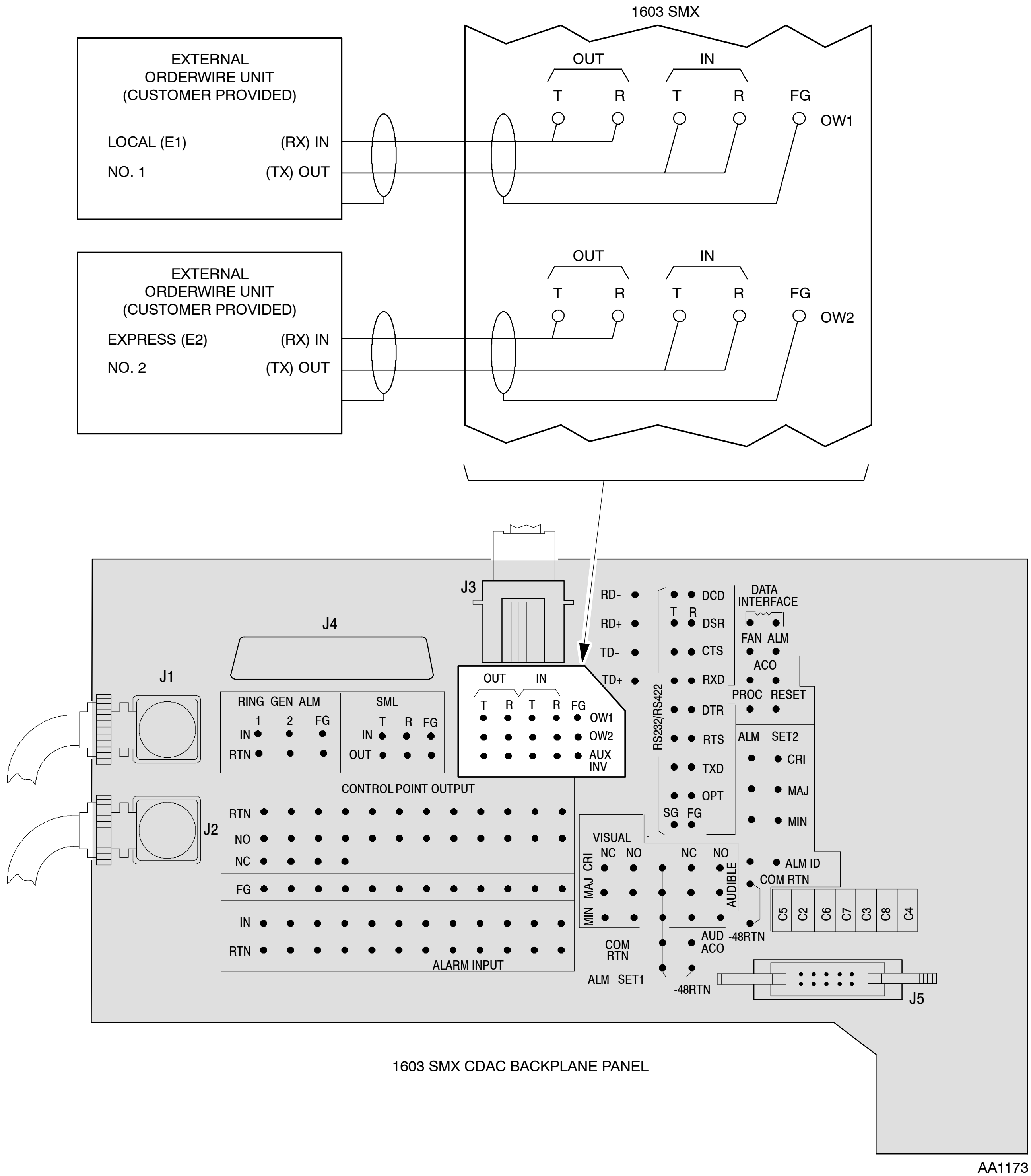


Figure 3. Orderwire Connections

7 Is RS-232 wiring for data terminal (DTE) or modem (DCE)?

If data terminal (DTE), go to step 8.
If modem (DCE), go to step 10.

8 Verify DTE wiring between RS-232 wire-wrap pins and terminating location. Table-A lists wiring terminations between backplane and DB-25 or DB-9 connector.

9 STOP. This procedure is complete.

Table A. Wiring to Data Terminal*

1603 SMX BACKPLANE	DATA TERMINAL CONNECTOR PINS	
	DB25	**DB9**
DCD-T	8	1
DSR-T	6	6
CTS-T	5	8
RXD-T	3	2
DTR-T	20	4
RTS-T	4	7
TXD-T	2	3
OPT-T	–	–
FG	–	–
SG	7	5

* *Typically, this application requires a female connector.*

10 ***NOTE:*** *Normal carrier detect operation sends a data carrier detect (DCD) signal to the Network Element (NE) craft port when it connects with another modem and drops DCD on disconnect. This method is recommended for security reasons (logon session is canceled when modem disconnects). If you want to leave logon session active when disconnected, choose No (DCD disabled) path.*

Do you want normal DCD operation, which is the recommended mode?

If yes, go to step 11.
If no (DCD disabled), go to step 13.

11 ***NOTE:*** *With DCD normal operation, craftport XON/XOFF flow control may be enabled when provisioning the port. XON/XOFF flow control is recommended when using the 1301 NMX.*

NOTE: *Some modem setup may be required to enable DCD operation. Refer to modem user's manual for setup information.*

Verify DCE wiring between RS-232 wire-wrap pins and modem. Table B lists wiring terminations between backplane and DB-25 or DB-9 connector.

12 STOP. This procedure is complete.

Table B. Craft 2 Port to Modem Wiring (Normal DCD Operation)*

1603 SMX BACKPLANE SIGNAL	DESCRIPTION	CONNECTOR TYPE		MODEM SIGNAL
		DB25	DB9	
DCD-T	Carrier Detect (RLSD)	–	–	
DSR-T	Data Set Ready	20	4	DTR
CTS-T	Clear To Send	4	7	RTS
RXD-T	Receive Data	2	3	TXD
DTR-T	Data Terminal Ready	8	1	DCD
RTS-T	Request To Send	5	8	CTS
TXD-T	Transmit Data	3	2	RXD
OPT-T	RXD Clock (Not used)	–	–	
FG	Frame Ground	–	–	
SG	Signal Ground	7	5	SG

* *Typically, this application requires a male connector.*

13 **NOTE:** *With DCD disabled operation, craftport XON/XOFF flow control should be disabled when provisioning port. Some modems locally echo while no carrier is present, which can result in craftport lockup if XON/XOFF flow control is enabled while DCD operation is disabled.*

Verify DCE wiring between RS-232 wire-wrap pins and modem. Table C lists wiring terminations between backplane and DB-25 or DB-9 connector.

14 STOP. This procedure is complete.

Table C. Craft 2 Port to Modem Wiring (DCD Disabled Operation)*

1603 SMX BACKPLANE SIGNAL	DESCRIPTION	CONNECTOR TYPE		MODEM SIGNAL
		DB25	DB9	
DCD-T	Carrier Detect (RLSD)	–	–	–
DSR-T	Data Set Ready	20	4	DTR
CTS-T	Clear To Send	4	7	RTS
RXD-T	Receive Data	2	3	TXD
DTR-T	Data Terminal Ready	6	6	DSR
RTS-T	Request To Send	5	8	CTS
TXD-T	Transmit Data	3	2	RXD
OPT-T	RXD Clock (Not used)	–	–	–
FG	Frame Ground	–	–	–
SG	Signal Ground	7	5	SG

* *Typically, this application requires a male connector.*

15 Locate RS-422 differential wire-wrap pins on shelf backplane (Figure 1).

16 Verify that cables (two 26 AWG, 100-ohm) run between the shelf and office TBOS subsystem.

17 Per Figure 4, verify that wire pairs properly terminate between backplane and TBOS subsystems.

18 Per Figure 4, verify that wire-wrap jumpers are in place between DTR-T, RTS-T and SG pins.

19 If other NE(s) share the TBOS interface, verify that the shelf's TBOS connections also run to the NE(s) (all wires to the same posts).

20 STOP. This procedure is complete.

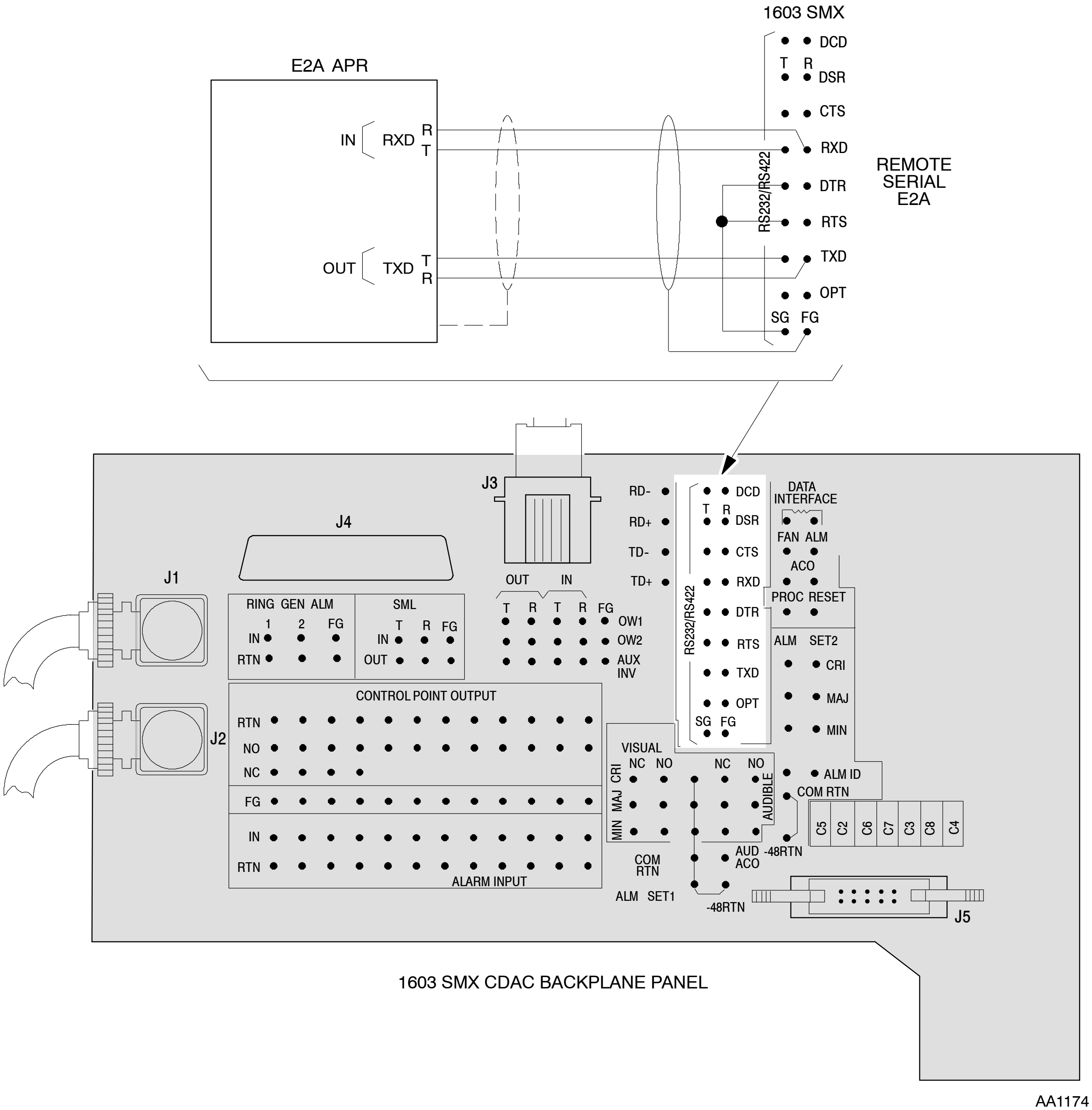


Figure 4. Typical Direct NE to TBOS Wiring

DLP-554
Restart Processor

Purpose

This procedure describes how to restart the processor on units that contain microprocessors.

STEP	PROCEDURE
1	In the scope pane, expand Equipment and select the equipment type (i.e., HIF, LIF, etc.) that you want to restart.
2	In the result pane, right-click the unit that you want to restart to display a context menu. **NOTE:** *Restarting the processor on the NEP logs you off the NE.*
3	From the context menu, select **Task>Operate>Restart Processor** to open a work view.
4	**CAUTION: Possibility of service interruption. Performing a "cold" restart may affect traffic.**
5	On the Processor Restart work view, select either Warm or Cold radio button. **NOTE:** *A "warm" restart is normally performed when there is a software problem. A "cold" restart is normally performed when there are both hardware and software problems.*
6	On the toolbar, select Submit icon. **NOTE:** *An Error dialog appears warning you that the operation will restart the selected processor. Select Yes to continue.*
7	After the restart completes, close the work view.
8	STOP. This procedure is complete.

DLP-555
Allow Remote Activation of VCL/VPL Continuity Checks

Purpose

This procedure describes how to remove an inhibit that is preventing the remote activation of a VCL or VPL connection continuity check or a segment continuity check.

STEP	PROCEDURE
1	In the scope pane, expand Facility; then expand USRLAN and select VCL or VPL.
2	In the result pane, select VCL (or VPL) on which you want to allow remote activation of a continuity check.
3	From the context menu that is displayed, select **Task>Provision>Allow/Inhibit** to display a Provision Allow/Inhibit work view.
4	Do you want to allow a connection continuity check or a segment continuity check? If connection continuity, then go to step 5. If segment continuity, then go to step 8.
5	From Activate Connection Continuity Check drop-down list, select Allow.
6	On the toolbar, select Submit icon; then close work view.
7	STOP. This procedure is complete.
8	From Activate Segment Continuity Check drop-down list, select Allow.
9	On the toolbar, select Submit icon; then close work view.
10	STOP. This procedure is complete.

DLP-556
Allow Remote Activation of VCL/VPL Performance Monitoring

Purpose

This procedure describes how to remove an inhibit that is preventing the remote activation of VCL/VPL connection or segment performance monitoring (PM).

STEP	PROCEDURE
1	In the scope pane, expand Facility; then expand USRLAN and select VCL or VPL.
2	In the result pane, right-click VCL (or VPL) that has PM inhibited to display a context menu.
3	From the context menu, select **Task>Provision>Allow/Inhibit** to display a Provision Allow/Inhibit work view.
4	Do you want to allow activation of connection PM or segment PM? If connection PM, then go to step 5. If segment PM, then go to step 8.
5	From the Activate Connection PM drop-down list, select Allow.
6	On the toolbar, select Submit icon; then close work view.
7	STOP. This procedure is complete.
8	From the Activate Segment PM drop-down list, select Allow.
9	On the toolbar, select Submit icon; then close work view.
10	STOP. This procedure is complete.

DLP-557
Retrieve/Change Provisioning for USRLAN Facility

Purpose

This procedure describes how to retrieve provisioned parameters for a USRLAN facility and how to change those parameters.

STEP	PROCEDURE
1	In the scope pane, expand Facility and select USRLAN.
2	In the result pane, right-click name of USRLAN facility (e.g., DG3-USRLAN-1-A) that you want to retrieve.
3	From the context menu that is displayed, select **Provision Parameters** to display a Provision Parameters work view.
4	On the work view, note how the parameters are provisioned.
5	Do you want to change any of the parameters? If yes, then go to step 6. If no, then go to step 8.
6	Click in the column under the parameter to display either a drop-down list or a spin box. For example, to change the Physical Layer parameter, click under Physical Layer and select either 10BASET, 100BASETX, or 1000BASELX.
7	On the toolbar, select Submit icon.
8	Close Provision Parameters work view.
9	STOP. This procedure is complete.

DLP-558
Allow Automatic Synchronization Restoration

Purpose

This procedure describes how to allow automatic restoration on NE sync and BITS sync entities.

STEP	PROCEDURE

1 Find the entity on which you want to allow automatic restoration in Table A.

Table A. Automatic Synchronization Restoration

IF YOU WANT TO...	THEN GO TO...
Allow automatic restoration on NE sync	Step 2
Allow automatic restoration on BITS sync	Step 9

Automatic Restoration of NE Sync

2 In the scope pane, expand System; then expand Synchronization and select NE Sync.

3 In the result pane, right-click NE Sync to display a context menu.

4 From the context menu, select **Task>Provision>Allow/Inhibit** to display a Provision Allow/Inhibit work view.

5 From the Auto Restoration drop-down list, select Allow.

6 On the work view toolbar, select Submit icon.

7 Close work view.

8 STOP. This procedure is complete.

Automatic Restoration of BITS Sync

9 In the scope pane, expand System; then expand Synchronization and select BITS Sync.

10 In the result pane, right-click BITS Sync A or B to display a context menu.

11 From the context menu, select **Task>Provision>Allow/Inhibit** to display a Provision Allow/Inhibit work view.

12 From the Auto Restoration drop-down list, select Allow.

13 On the work view toolbar, select Submit icon.

14 Close work view.

15 STOP. This procedure is complete.

DLP-559
Retrieve/Change ATM Cell Encapsulation

Purpose

This procedure describes how to retrieve and change ATM cell encapsulation provisioning.

STEP	PROCEDURE
1	In the scope pane, expand Facility.
2	Expand USRLAN and select AAL5.
3	In the result pane, right-click AAL5 facility you want to check to display a context menu.
4	From the context menu, select **Provision Parameters** to display a Provision Parameters work view.
5	In the ATM Cell Encapsulation Type field, note how encapsulation is provisioned.
6	Do you want to change the provisioned value? If yes, then continue to step 7. If no, then go to step 9.
7	From the ATM Cell Encapsulation Type drop-down list, select either Off or RFC1483.
8	On the work view toolbar, select Submit icon.
9	Close work view.
10	STOP. This procedure is complete.

DLP-560
Retrieve Direct Neighbors

Purpose

This procedure describes how to retrieve direct neighbors.

STEP	PROCEDURE
1	In the scope pane, expand System.
2	Expand Network Features and select NSAP.
3	In the result pane, right-click Direct Neighbors to display a context menu.
4	From the context menu, select **View** to display a work view.
5	After identifying direct neighbors, close work view.
6	STOP. This procedure is complete.

DLP-561
Retrieve/Change E2A Map Provisioning

Purpose

This procedure describes how to retrieve and change E2A Map provisioning.

STEP	PROCEDURE
1	In the scope pane, expand System.
2	Expand Network Features and select E2A Map.
3	Select either Remote or Concentrator.
4	In the result pane, right-click CONC or E2AMAP-x to display a context menu.
5	From the context menu, select **Provision** to open a work view.
6	Note the name of the remote NE.
7	Do you want to change the name? If yes, go to step 8. If no, go to step 10.
8	Enter the new NE name in the Remote NE Name text field.
9	On the toolbar, select Submit icon.
10	Close the work view.
11	STOP. This procedure is complete.

DLP-562
Retrieve/Change RAD Map Provisioning

Purpose

This procedure describes how to retrieve and change RAD Map provisioning.

STEP	PROCEDURE
1	In the scope pane, expand System.
2	Expand Network Features and expand RAD Map.
3	Select either Remote or Concentrator.
4	In the result pane, right-click CONC-x or RADMAP-x to display a context menu.
5	From the context menu, select **Provision** a open a work view.
6	Note the provisioned data on the work view.
7	Do you want to change an entry? If yes, go to step 8. If no, go to step 10.
8	To change the Remote NE Name enter the new name in the text field. To change the provisioned value for Far End Display Enabled, select either Disabled or Enabled from the drop-down list.
9	On the toolbar, select Submit icon.
10	Close the work view.
11	STOP. This procedure is complete.

DLP-563
Retrieve/Change BLSR Manual Sequence Map Provisioning

Purpose

This procedure describes how to retrieve the manual BLSR Sequence Map and if necessary how to change entries in the map.

STEP	PROCEDURE
1	In the scope pane, expand BLSR.
2	Expand Sequence Map and select Manual Map.
3	In the result pane, right-click Manual Map to display a context menu.
4	From the context menu, select **Provision Parameters** to display a work view.
5	Note the provisioned data for the sequence map.
6	Do you want to change any entries on the sequence map? If yes, go to step 7. If no, go to step 9.
7	Use the drop-down lists to change values that are not correct.
8	On the toolbar, select Submit icon.
9	Close the work view.
10	STOP. This procedure is complete.

DLP-564
Retrieve BLSR Automatic Sequence Map

Purpose

This procedure describes how to retrieve the BLSR Automatic Sequence Map.

STEP	PROCEDURE
1	In the scope pane, expand BLSR.
2	Expand Sequence Map and select Automatic Map.
3	In the result pane, note the NEs that are in the BLSR ring.
4	STOP. This procedure is complete.

DLP-565
Identify LDR501 Carrying Alarmed Path or Facility

Purpose

This procedure describes how to identify the LDR501 that is carrying an alarmed path or alarmed facility. It also explains how to determine the physical location of that LDR501 in the main shelf or in a facility expansion shelf (FES).

- If alarmed path is an STS1 path, go to step 1.
- If alarmed facility is a DS3 facility, go to step 4.
- If alarmed path is a VT1 path, go to step 7.
- If alarmed facility is an EC1 facility, go to step 10.

STEP	PROCEDURE

STS1 Path

1 Find the AID of the STS1 path that is generating the alarm in the first or third column in Table A.

Table A. STS1 Path-to-LDR Assignments

IF STS1 PATH AID IS...	THEN LDR AID IS...	IF STS1 PATH AID IS...	THEN LDR AID IS...
DGx-STS1-1*	DGx-GRP1-LDR-1	DGx-STS1-7	DGx-GRP2-LDR-1
DGx-STS1-2	DGx-GRP1-LDR-1	DGx-STS1-8	DGx-GRP2-LDR-1
DGx-STS1-3	DGx-GRP1-LDR-2	DGx-STS1-9	DGx-GRP2-LDR-2
DGx-STS1-4	DGx-GRP1-LDR-2	DGx-STS1-10	DGx-GRP2-LDR-2
DGx-STS1-5	DGx-GRP1-LDR-3	DGx-STS1-11	DGx-GRP2-LDR-3
DGx-STS1-6	DGx-GRP1-LDR-3	DGx-STS1-12	DGx-GRP2-LDR-3
* *x=1, 2, 3, or 4*			

2 In the second or fourth column, note the AID of the LDR that is associated with that path.

For example, if the AID in the alarm message is DG1-STS1-7, the AID of the LDR carrying that STS1 path is DG1-GRP2-LDR-1. The physical location of the LDR is the first working slot (LDR-1) of Group 2 in Drop Group 1. See Figure 1.

3 STOP. This procedure is complete.

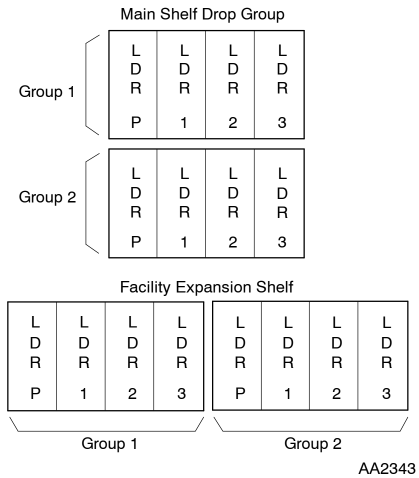


Figure 1. LDR501 Locations in Main Shelf and Facility Expansion Shelf (FES)

DS3 Facility

4 Find the AID of the DS3 facility that is generating the alarm in the first or third column in Table B.

Table B. DS3 Facility-to-LDR Assignments

IF DS3 AID IS...	THEN LDR AID IS...	IF DS3 AID IS...	THEN LDR AID IS...
DGx-DS3-1*	DGx-GRP1-LDR-1	DGx-DS3-7	DGx-GRP2-LDR-1
DGx-DS3-2	DGx-GRP1-LDR-1	DGx-DS3-8	DGx-GRP2-LDR-1
DGx-DS3-3	DGx-GRP1-LDR-2	DGx-DS3-9	DGx-GRP2-LDR-2
DGx-DS3-4	DGx-GRP1-LDR-2	DGx-DS3-10	DGx-GRP2-LDR-2
DGx-DS3-5	DGx-GRP1-LDR-3	DGx-DS3-11	DGx-GRP2-LDR-3
DGx-DS3-6	DGx-GRP1-LDR-3	DGx-DS3-12	DGx-GRP2-LDR-3
* *x=1, 2, 3, or 4*			

5 In the second or fourth column, note the AID of the LDR that is associated with that facility.

For example, if the AID in the alarm message is DG4-DS3-5, the AID of the LDR carrying that facility is DG4-GRP1-LDR-3. The physical location of the LDR is the third working slot (LDR-3) of Group 1 in Drop Group 4. See Figure 1.

6 STOP. This procedure is complete.

VT1 Path

7 Find the AID of the VT1 path that is generating the alarm in the first or third column in Table C.

Table C. VT1 Path-to-LDR Assignments[4]

IF VT1 PATH AID IS...	THEN LDR AID IS...	IF VT1 PATH AID IS...	THEN LDR AID IS...
DGx-VT1-1-vtpath[5]	DGx-GRP1-LDR-1	DGx-VT1-7-vtpath	DGx-GRP2-LDR-1
DGx-VT1-2-vtpath	DGx-GRP1-LDR-1	DGx-VT1-8-vtpath	DGx-GRP2-LDR-1
DGx-VT1-3-vtpath	DGx-GRP1-LDR-2	DGx-VT1-9-vtpath	DGx-GRP2-LDR-2
DGx-VT1-4-vtpath	DGx-GRP1-LDR-2	DGx-VT1-10-vtpath	DGx-GRP2-LDR-2
DGx-VT1-5-vtpath	DGx-GRP1-LDR-3	DGx-VT1-11-vtpath	DGx-GRP2-LDR-3
DGx-VT1-6-vtpath	DGx-GRP1-LDR-3	DGx-VT1-12-vtpath	DGx-GRP2-LDR-3

[4] *The VT numbering format shown in the VT path AIDs is sequential numbering. A VT path AID with grouped numbering format would appear as DGx-VT1-4-vtgrp-vt.*

[5] *x=1, 2, 3, or 4*
vtpath=1...28

8 In the second or fourth column, note the AID of the LDR that is associated with that path.

For example, if the AID in the alarm message is DG2-VT1-9-18, the AID of the LDR carrying that path is DG2-GRP2-LDR-2. The physical location of the LDR is the second working slot (LDR-2) of Group 2 in Drop Group 2. See Figure 1.

9 STOP. This procedure is complete.

EC1 Facility

10 Find the AID of the EC1 facility that is generating the alarm in the first or third column in Table D.

11 In the second or fourth column, note the AID of the LDR that is associated with that facility.

For example, if the AID in the alarm message is DG3-EC1-3, the AID of the LDR carrying that facility is DG3-GRP1-LDR-2. The physical location of the LDR is the second working slot (LDR-2) of Group 1 in Drop Group 3. See Figure 1.

Table D. Facility-to-LDR Assignments

IF EC1 AID IS...	THEN LDR AID IS...	IF EC1 AID IS...	THEN LDR AID IS...
DGx-EC1-1*	DGx-GRP1-LDR-1	DGx-EC1-7	DGx-GRP2-LDR-1
DGx-EC1-2	DGx-GRP1-LDR-1	DGx-EC1-8	DGx-GRP2-LDR-1
DGx-EC1-3	DGx-GRP1-LDR-2	DGx-EC1-9	DGx-GRP2-LDR-2
DGx-EC1-4	DGx-GRP1-LDR-2	DGx-EC1-10	DGx-GRP2-LDR-2
DGx-EC1-5	DGx-GRP1-LDR-3	DGx-EC1-11	DGx-GRP2-LDR-3
DGx-EC1-6	DGx-GRP1-LDR-3	DGx-EC1-12	DGx-GRP2-LDR-3
* *x=1, 2, 3, or 4*			

12 STOP. This procedure is complete.

DLP-566
Download Software From PC to Processor-Controlled Units

Purpose

This procedure describes how to download program kit software to processor-controlled units in the NE.

Prerequisite

A PC containing the download software must be connected to the craft port on the front of the COA via an RS-232 cable.

STEP	PROCEDURE
1	**CAUTION: Possibility of service interruption. Do not interrupt the download process once it has begun (i.e., press keys on keyboard, insert/remove units, remove power, remove craft port cable, etc.).**
2	In the scope pane, right-click NE name to display a context menu.
3	From the context menu, select **Task>Download>Processor** to open a work view.
4	From the Download Release drop-down list on the work view, select the software release you want to download.
5	Select the unit to be downloaded from the list of units. **NOTE:** *The unit selected must be assigned and cannot have an MEA (mismatched equipment) alarm.*
6	On the toolbar, select Submit icon to start download process. **NOTE:** *After initiating the download process, the message, Erasing processor memory.., is displayed for 15 seconds to 1 minute. After this step is completed, the message, Downloading ..., is displayed. This step takes 30 seconds to 3 minutes to complete. The size of the processor being downloaded determines the length of time.* **NOTE:** *During the download, the ACT LED also flashes on the target processor. If necessary, refer to Tables A, B, and C for download error, warning, and informational messages.*

7 If you are downloading software to other processor units, repeat from step 4.

8 After downloads are completed, close the work view.

9 STOP. This procedure is complete.

Table A. Download Error Messages

TEXT	CAUSE	SOLUTION
Selected processor not supported by selected release (status bar message).	There is no software file in the selected download release for the processor type in the Processor Status box.	Select another release.
Selected processor is unassigned (status bar message).	The processor selected in the processor status list box is unassigned (UAS) and, therefore, is of an unknown type.	Go to appropriate provisioning screen and assign the processor.
No response from NE.	Communication with the NE was interrupted while downloading.	Check serial cable; try download again. If message reappears, retry download.
NE memory failure.	The NE encountered an error attempting to program Flash memory.	Try download again; replace plug-in unit if error persists.
Initialization failed.	Communication could not be established with bootcode, or the target processor reported a memory failure while attempting to erase Flash memory.	Try download again.
Download failed. Do not remove power from target processor while its ACT (green) LED is flashing.	Download record transfer was interrupted prior to completion of download.	Try download again.
Download failed. The NEP takes a few minutes to initialize. Wait for the ACT (green) LED to stop blinking before attempting to download the NEP again.	Download to the NEP failed.	Try download again.
Selected release data is corrupt.	An error occurred when reading a software image file of the selected software release.	Reinstall the 1603 SMX program kit on the PC.

Table B. Download Warning Messages

TEXT	CAUSE	SOLUTION
Upgrade to selected release is not recommended since it may result in loss of provisioning data. Do you want to download the selected release?	A release has been selected in the download release box which is not upgrade-compatible with the current software version on the NEP.	Unless reverting to a prior release, recommend that user select NO and select another release in Download Release box.
Selected release cannot be downloaded to this NE (status bar message).	Cannot upgrade directly from Release xx.xx to Release yy.yy or later releases.	Upgrade to Release xx.xx first per Guide to Upgrading manual.

Table C. Download Informational Messages

TEXT	CAUSE
Download completed.	Download record transfer completed normally.
Download completed. The NEP takes a few minutes to initialize. Rediscover the local NE after the NEP restarts to continue with the upgrade process.	Download of NEP completed normally.
You will be logged off of the local NE now.	The user has selected Close after successfully downloading.

10 STOP. This procedure is complete.

DLP-567
Connect PC or VDT to Craft 1 or Craft 2 Port

Purpose

This procedure describes how to connect a Personal Computer (PC) or Video Display Terminal (VDT) to a Craft 1 or Craft 2 port.

STEP	PROCEDURE
1	Are you connecting to Craft 1 (USI) port or Craft 2 port (backplane)? If Craft 1, go to step 2. If Craft 2, go to step 8.
2	See Figure 1 for location of Craft 1 port.
3	**NOTE:** *For PC or VDT with 25-pin male RS-232 port, use 601229-540-072 9-pin male to 25-pin female cable assembly, or equivalent.* **NOTE:** *For PC or VDT with 25-pin female RS-232 port, use 601154-540-072 9-pin male to 25-pin male cable assembly, or equivalent.* **NOTE:** *For PC or VDT with 9-pin RS-232 port, use 695-7683-033 9-pin male to 9-pin female cable assembly, or as required.* Obtain RS-232 cable to connect PC or VDT to 9-pin female connector on COA. See Figure 2 for recommended cable wiring.
4	If using cable with ground wire, connect ground wire to ground post on shelf (Figure 1).
5	Use a small flat head screwdriver to connect the 9-pin connector end of cable to COA front connector. Connect the other end of the cable to the VDT or PC serial port.
6	Refer to DLP-117 to log on to the NE.
7	STOP. This procedure is complete.

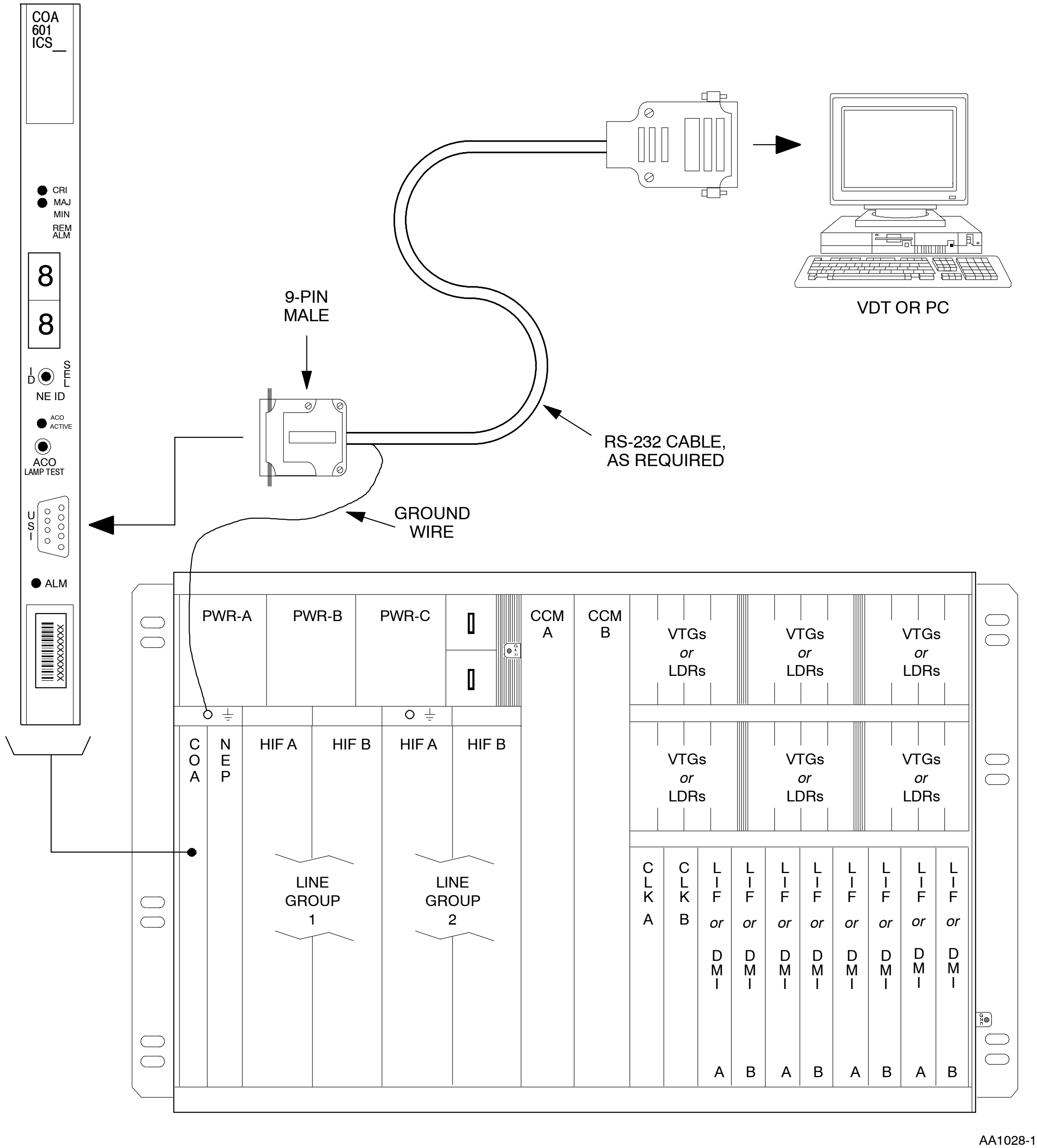


Figure 1. Connecting Craft Terminal (VDT or PC) to Craft 1 (USI) Port

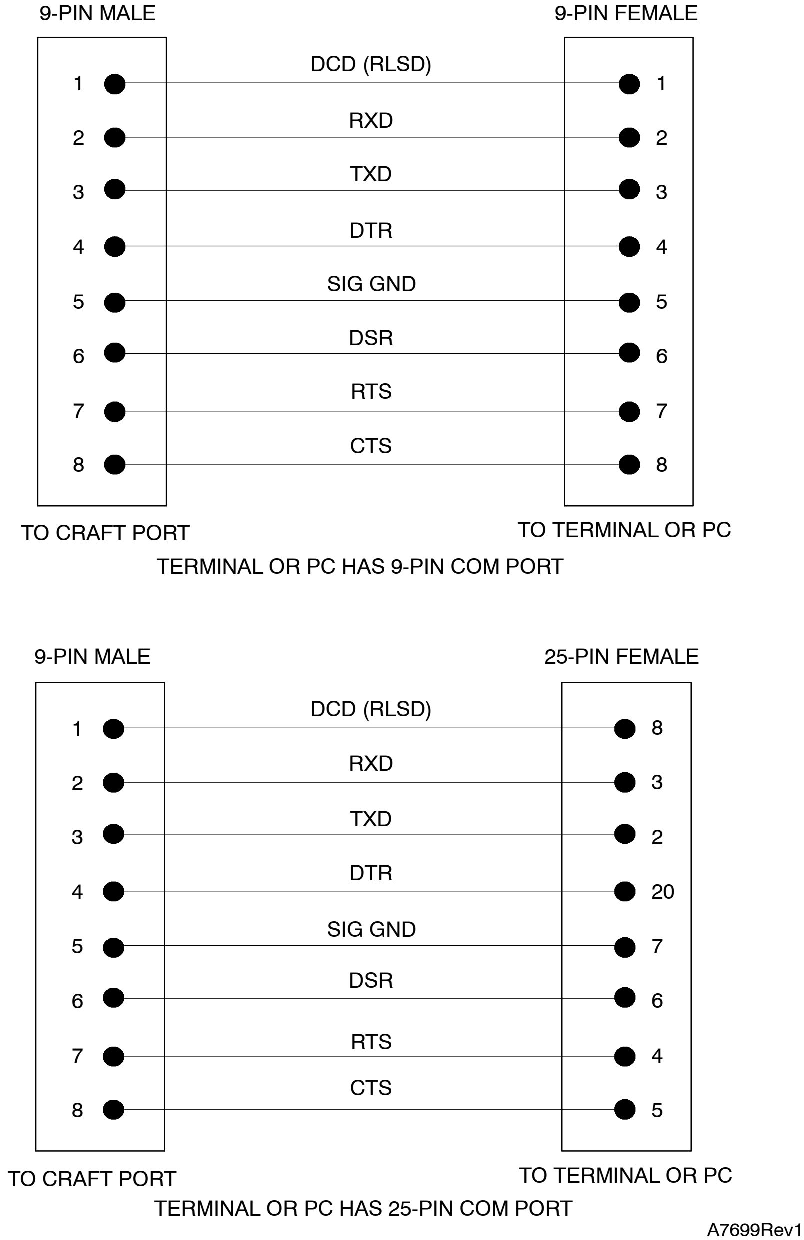


Figure 2. Craft 1 (USI) Port Interface Cable Wiring

8 ***NOTE:*** *The Craft 2 (RS-232) interface requires odd-numbered COA units.*

Verify RS-232 wiring from terminal or PC to 1603 SMX backplane per DLP-008.

9 Assign the Craft 2 port:

a. In the scope pane, expand System; then expand Ports; then expand Craft 2 and select RS232.

b. In the result pane, right-click RS232 to display a context menu.

c. From the context menu, select **Provision Parameters** to open a work view.

d. From the Service State drop-down list, select In Service.

e. On the toolbar, select Submit; then close work view.

10 Refer to DLP-117 and TNG-503 to log on to the NE.

11 STOP. This procedure is complete.

DLP-568
Copy Software Program (Local Only)

Purpose

This procedure describes how to locally copy program software between devices in the same NE.

General

This procedure addresses copying program software between devices located in the same Network Element (NE). Copying program images between different NEs (i.e., remote download) is described in DLP-569.

Prerequisites

- The target processor is assigned.
- The target processor does not have an MEA, INVERR, or CONTCOM alarm condition.
- A valid source is available on program backup COA or from another processor of the same type. The software version of the source processor or program backup must match the NEP software version.

STEP	PROCEDURE
1	Is NE equipped with COA with expanded memory (COA603-610)? If yes, go to step 5. If no, go to step 2.
2	If necessary, determine if a valid software image source is available: a. In the scope pane, expand System and select Inventory. b. In the result pane, right-click Software Inventory to display a context menu. c. From the context menu, select **View** to open a work view.
3	Is a valid source with software loaded available per Table A? If yes, go to step 5. If no, go to step 4.
4	Download software from PC [DLP-566].

5 Refer to Tables A and B for valid combinations of From and To devices.

Table A. Compatible Devices for Copy Program – Local

SOURCE DEVICE	COMPATIBLE DESTINATION DEVICES	COMMENTS
COM	All	COM only applies if NE is equipped with Program Backup COA (with appropriate program load).
CCM101	CCM101	
DMI101	DMI101	
DMI301	DMI301	
HIFB0x, HIFC0x	HIFB0x, HIFC0x, HIF60x, HIF70x, HIF90x, and HIFA0x	
HIF60x, HIF70x, HIF90x, HIFA0x	HIFB0x, HIFC0x, HIF60x, HIF70x, HIF90x, and HIFA0x	
HIFF0x	HIFF0x	
HIFH0x, HIFJAx, HIFJBx, HIFJCx, HIFJDx, HIFJEx HIFJFx	HIFF0x	
LIF20x	LIF20x	
LIF30x	LIF30x	
LIF40x	LIF40x, LIFA0x, or LIFH0x	
LIF50x/701	LIF50x and LIF701	
LIF601	LIF601	
LIF901	LIF901	
LIFA0x/LIFH0x	LIFA0x, LIF40x, or LIFH0x	
LIFD01	LIFD01	
LIFF01	LIFF01	
NEP60x	None	
CCM201	CCM201	
LIFG01	LIFG01	

Table B. 1301 NMX Valid Combinations for Copy Program – Local

OPERATION	FROM DEVICE	TO DEVICE
Download from specified source to one destination. Does not include NEP	Specific source processor	Specific target processor
Download from Program Backup to one destination which may include NEP	Backup (COM)	Specific target processor
Valid source image (which may be Program Backup) is determined by system for specified destination, which may be NEP	Auto Select	Specific target processor
Valid source images are determined by system for each possible destination not including NEP	Auto Select	ALL-A or ALL-B

6 Copy software image from one device to another:

a. In the scope pane, right-click NE name to display a context menu.

b. From the context menu, select **Task>Download>Copy Program Local** to open a work view.

c. In the Copy To region on the work view, select the target unit.

d. From the Copy From drop-down list, select the device you want to use as the source or select Auto Select.

e. On the toolbar, select Submit icon to start the copy process.

NOTE: *The green ACT (active) LED on the source and target devices flash during the copy process and stop flashing when the process completes.*

f. Close work view.

7 STOP. This procedure is complete.

DLP-569
Remotely Download Software From Another NE

Purpose

This procedure describes how to download software to the local NE from another NE in the network

STEP	PROCEDURE
1	In the scope pane, right-click NE name to display a context menu.
2	From the context menu, select **Task>Download>Copy Program Remote** to open a work view.
3	On the work view, enter the TID of the source NE in the From NE TID field.
4	Enter the type of software being downloaded in the Type field (e.g., ADR48).
5	Enter the software version in the Release field.
6	On the toolbar, select Submit to start the download.
7	Wait until the download completes (approximately 20 minutes).
8	Close the work view.
9	STOP. This procedure is complete.

DLP-570
Download Software to Directly Connected NE

Purpose

This procedure describes how to download software from a PC directly to the COA on a local NE.

STEP	PROCEDURE
1	In the scope pane, right-click NE name to display a context menu.
2	From the context menu, select **Task>Download>Storage Unit** to open a work view.
3	From the Download Release drop-down list, select the software release. **NOTE:** *The work view displays the current software releases installed on the COA in the Current Storage Unit Contents field.*
4	On the toolbar, select Submit to start the download. **NOTE:** *The ACT LED on the NEP starts flashing and flashes continually until the download is completed. Also a Download Progress dialog on the PC identifies the files that are being downloaded and a progress bar tracks the download of each file.*
5	Wait until the download process completes (approximately 30 minutes). **NOTE:** *The green LED on the NEP stops flashing when the download process is complete.* **NOTE:** *At the end of the download, the Current Storage Unit Contents field displays the new software load.*
6	Close the work view.
7	STOP. This procedure is complete.

DLP-571
Perform FTP Backup of Provisioning Database

Purpose

This procedure describes how to perform an FTP backup of provisioning data from an NE to a PC.

Prerequisites

To perform this procedure, the NE being backed up must have IP-based access (i.e., via a LAN, a PPP connection, or an EMG IP tunnel).

STEP	PROCEDURE
1	In the scope pane, right-click NE name to display a context menu.
2	From the context menu, select **Task>Backup/Restore>FTP Backup** to open a work view.
3	Is the NE being backed up the gateway NE? If yes, then go to 5. If no, then go to 4.
4	**NOTE:** *The TID of the gateway NE appears in the TID field in the Relay Node region, but you must enter a User ID and Password.* Enter User ID and Password.
5	**NOTE:** *On the work view, you can enter a file name for the backup file directly in the Save File edit box or you can open a File Save dialog to create the file name.* Do you want to open a File Save dialog? If yes, then go to step 9. If no, then go to step 6.
6	In the Save File field on the work view, enter the name of the file in which the retrieved data will be stored. **NOTE:** *A .bkp extension is required on the file name.*
7	Enter a description of the file contents in the Enter File Note field (e.g., NE name, date/time, software version, etc.).

8 On the toolbar, select the Submit icon to start the backup process; then go to step 14.

9 In the Save File region of the work view, click the Browse button to open a File Save As dialog.

10 ***NOTE:*** *On the Save As dialog, the File name defaults to the TID of the NE being backed up.*

From the Save as type drop-down list, select Backup Files.

11 Click the Save button to return to the Backup work view.

NOTE: *If the file name you selected already exists, a message is displayed warning you that the file will be overwritten.*

12 ***NOTE:*** *The name of the file you selected appears in the Save File field on the work view.*

Enter a description of the file contents in the Enter File Note field (e.g., NE name, date/time, software version, etc.).

13 On the toolbar, select the Submit icon to start the backup process.

14 ***NOTE:*** *A progress bar is displayed while the backup is taking place.*

When the “Backup Operation is complete” message appears, click OK.

15 Close the work view.

16 STOP. This procedure is complete.

DLP-572
Perform FTP Restoral of Provisioning Database

Purpose

This procedure describes how to restore backedup provisioning data from a PC to an NE.

Prerequisites

To perform this procedure, access to the NE being restored must be IP-based (i.e., via a LAN, a PPP connection, or an EMG IP tunnel).

STEP	PROCEDURE
1	In the scope pane, right-click NE name to display a context menu.
2	From the context menu, select **Task>Backup/Restore>FTP Restore** to open a work view.
3	Is the NE being restored the gateway NE? If yes, then go to 5. If no, then go to 4.
4	***NOTE:*** *The TID of the gateway NE appears in the TID field in the Relay Node region, but you must enter a User ID and Password.* Enter User ID and Password.
5	***NOTE:*** *On the work view, you can enter the file name of the backup file directly in the File Selection edit box or you can open an Open File dialog to retrieve the backup file.* Do you want to open an Open File dialog? If yes, then go to step 8. If no, then go to step 6.
6	In the File Selection edit box on the work view, enter the name of the file being retrieved. ***NOTE:*** *The file name contains a .bkp extension.*
7	On the toolbar, select the Submit icon to start the backup process; then go to step 12.

8 In the File Selection region of the work view, click the Browse button to open an Open File dialog.

9 From the List files of type drop-down list, select the backup file.

10 Click OK to return to the Restore NE work view.

11 **NOTE:** *The name of the file you are restoring appears in the File Selection field on the work view.*

On the toolbar, select the Submit icon to start the restore process.

12 **NOTE:** *A progress bar is displayed while the restore process, which is an FTP transfer, is taking place. The data being transferred is placed in the Secondary database on the NEP.*

Wait for the restore process to complete.

13 **NOTE:** *After all the data has been transferred, the 1301 NMX initiates a CPY-MEM command to copy the provisioning data from the Secondary database to the Primary database. When the copy completes, a message displays indicating that a cold restart will be performed and you must log off and log back on in order to use the new provisioning data.*

Log off the NE.

14 After the restart completes, log on to the NE.

NOTE: *The cold restart deletes the provisioning data that was in the Secondary database.*

15 STOP. This procedure is complete.

DLP-573
Allow Fast Facility Protection (FFP) Switch

Purpose

This procedure describes how to allow a Fast Facility Protection (FFP) switch when testing OCn protection switching.

STEP	PROCEDURE
1	In the scope pane, expand System; then expand General and select Global Settings.
2	In the result pane, right-click Global Settings to display a context menu.
3	From the context menu, select **Provision Parameters-NE** to open a work view.
4	In the NE Allow/Inhibit region on the work view, select Allow from the OCn Fast Switch drop-down list.
5	On the toolbar, select Submit icon.
6	Close work view.
7	STOP. This procedure is complete.

DLP-574
Change POS Port PM Threshold Level

Purpose

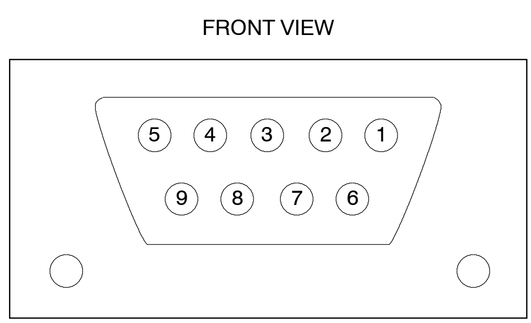
This procedure describes how to change POS Port PM threshold levels.

STEP	PROCEDURE
1	In the scope pane, expand Facility; then expand USRLAN and select POS Port.
2	In the result pane, right-click POS Port for which PM information is being changed to display a context menu.
3	From the context menu, select **Task>Provision>PM Threshold** to open a work view.
4	In the Name column, find the threshold you want to change (e.g., ABTPKT, FCSERR, etc.) and use the spin-box in the 15-Minute or 1-Day Value column to change the value.
5	On the toolbar, select Submit icon.
6	Close work view.
7	STOP. This procedure is complete.

TNG-503
Craft Interface Operation and Conventions

1. Local Access

1.1 The basic means for locally interfacing with the 1603 SMX system is provided by the Craft, Orderwire, and Alarm plug-in unit (COAxxx). On the front panel of the COA is a 9-pin subminiature D connector (marked USI) that serves as the Craft 1 (RS-232) access port. Figure 1 shows the pin configuration of the connector. Figure 2 shows the recommended cable connections for 9-pin and 25-pin terminal/PC serial ports. Alcatel cable 601229-540-072 provides 9-pin male to 25-pin female configuration, and 695-7683-033 provides 9-pin male to 9-pin female configuration. For a more permanent connection, a second craft port with wire-wrap pins is on the shelf backplane (see Remote Access).



PIN NUMBER	DESCRIPTION
1	DCD
2	RXD
3	TXD
4	DTR
5	SGND
6	DSR
7	RTS
8	CTS
9	OPTIONAL

A5627

Figure 1. COAxxx USI RS-232 Connector, Front View

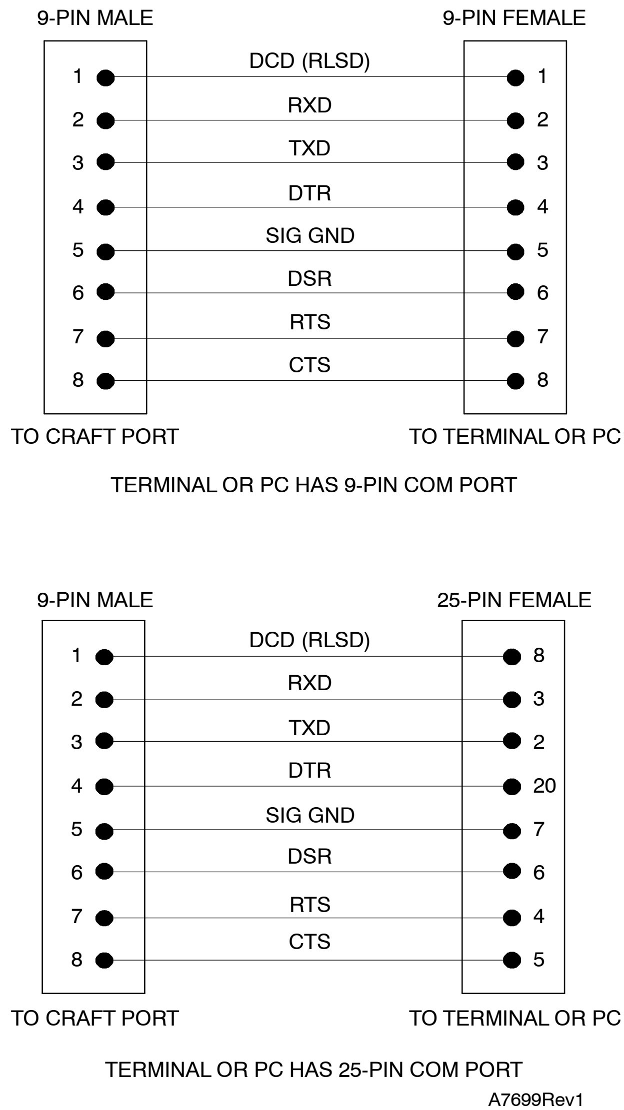


Figure 2. Craft 1 Port Interface Cable Wiring

1.2 To access the 1603 SMX through the Craft 1 port, an IBM or compatible Personal Computer (PC) with an available RS-232 serial port is required. The 1301 NMX software provides the user interface for provisioning and alarm monitoring activities through the PC serial port to the Craft 1 port. The default communications parameters of the 1603 SMX Network Element and the 1301 NMX software communications driver are:

Baud rate:	9600
Number of bits:	8
Parity:	None
Stop bits:	1
Line width (characters):	80

1.3 When the COA is accessed, the baud rate can be changed to 300, 1200, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 57600, 115200, or AUTO_BAUD. However, a baud rate change does not take effect until after the user logs off and logs back on to the NE. To regain access, the PC must be reset to the new parameters. AUTO_BAUD is not recommended with the 1301 NMX software program.

2. Remote Access

2.1 There are two methods for remotely logging on to an NE. One method is using a modem connected to the RS-232 wire-wrap pins on the shelf backplane. This is the Craft 2 port and requires the COAx01, x03, or x05 plug-in unit. As far as the NE is concerned, this is a second local craft port. The Craft 2 port could be wired to a VDT instead of a modem for a permanent local craft interface.

2.2 The second method of remotely logging on to an NE allows a user to connect to one NE (the local NE) and request a logon session on another NE (the remote NE).

2.3 To remotely log on to an NE over the SONET Embedded Communication Channel (EOC), do the following: in the NMX Explorer application window result pane, find the NE in the list of NEs; right-click the NE to display a context menu; on the context menu, select Logon; enter your User Name and Password and select OK.

3. Serial E2A Interface

3.1 Even numbered COAs, (i.e., COAx02, x04, x06, etc.), provide a differential RS-422 interface in place of the RS-232 Craft 2 port that is on odd numbered COAs (COAx01, x03, x05, or x07). The RS-422 port is intended for a serial E2A interface that supports the Telemetry Byte-Oriented Serial (TBOS) protocol. Like the odd numbered COAs, this port is accessed using the wire-wrap pins on the shelf backplane. An odd numbered COA can be used for a serial E2A interface if an RS-232 interface is required instead of an RS-422 interface.

4. Conventions For Entering Commands From The 1301 NMX

4.1 The 1301 NMX procedures in this manual assume the user is logged on to the 1603 SMX Network Element through the 1301 NMX Explorer software program and has opened the 1603 SMX Application browser. Familiarity with the 1301 NMX user environment is necessary for using this manual.

4.2 The 1603 SMX Application browser provides access to individual work views where commands are initiated to affect the 1603 SMX Network Element. The 1603 SMX Application browser is available after logging on the Network Element. Refer to DLP-117 to log on the Network Element.

4.3 A command is issued from a work view by selecting options from drop-down lists, spin boxes, etc., and then submitting these changes.

4.4 To access a work view, make selections in the scope pane, result pane, and from a context menu.

4.5 For more information about the components of the work views, refer to the 1301 NMX User's Guide for 1603 SMX.

TNG-507
Alarms, Conditions, and Events

1. General

General Description

1.1 This section provides tables that summarize the provisionable and nonprovisionable characteristics of the condition types used by the 1603 SMX. Condition types help the craftperson isolate the type of error to minimize trouble-clearing delays. These tables should prove most useful after initial provisioning. (See the Provisioning Guide.)

1.2 When errors are detected by the system, the craftperson is notified by lighted LED alarm lamps, by retrieving current alarm conditions using the 1301 NMX, or by receiving automatically generated system status and event reporting through autonomous messages.

COA Alarm Level Notification LEDs

1.3 When alarm conditions cause the LED COA alarm level notification lamps to activate, the lamps represent the severity level of the current alarms. Critical (CR) and Major (MJ) alarms display a red lamp and Minor (MN) alarms display a yellow lamp. The warning light deactivates when the alarm condition is corrected.

Retrieving Current Status of Alarms and Conditions

1.4 Provisionable alarm conditions have associated notification codes with varying degrees of severity. Although these alarms have default notification codes, most codes can be changed using the set attribute (SET-ATTR-<*xxx*>) TL1 commands, where <*xxx*> represents the entity associated with the alarm condition. Once the notification codes are set, the current alarm conditions can be retrieved at any time using the retrieve alarm (RTRV-ALM-<*xxx*>) and retrieve condition (RTRV-COND-<*xxx*>) TL1 commands for an entity. Refer to Table A for the standard alarm notification codes.

Table A. Standard Alarm Notification Codes

NOTIFICATION CODE	DESCRIPTION
CR	Critical Alarm
MJ	Major Alarm
MN	Minor Alarm
NA	Not Alarmed. Reported as an event and retrieved as a condition
NR	Not Reported. Retrieved as a condition

Retrieving Autonomous Messages

1.5 Autonomous messages are automatically generated as they occur. These messages report nonalarmed events and also report when alarms clear. Accumulated autonomous messages can be reviewed using either the RTRV-LOG or RTRV-AO TL1 command. The RTRV-LOG command saves the autonomous messages in a message log and sorts them as either system or security messages. The RTRV-AO command provides additional filtering capabilities to retrieve messages (except CAMR) from the system log based on ATAG, autonomous message type, and/or the database change report sequence.

1.6 Refer to Table B for the autonomous message types categories.

Table B. Autonomous Message Categories

MESSAGE TYPE	CATEGORY
ALM	Alarmed
DBCHG	NE Database Change has occurred
EVT	Event
EX	Exercise
PM	Performance Monitoring report
RMV	Remove (entity placed in OOS-MT maintenance state)
RST	Restore (entity returned to In-Service state from OOS-MT)
SW	Switch (entity has switched to/from protection)

Table Description

1.7 The tables in this section are organized by entities that are valid for the 1603 SMX. Each condition type is listed with the default notification code values, service-affecting/nonservice-affecting behavior codes, short-text descriptions, LED plug-in units that respond with the alarm (if applicable), and the Serial E2A bit (if applicable).

Default Notification Code (NTFCNCDE)

1.8 In the following tables, the default notification code column lists the default alarm notification codes for the active (ACT) and standby (STBY) sides of the equipment or facility. (If the entity is not duplex, only the ACT notification code is applicable.) Most notification codes may be changed by the SET-ATTR TL1 command for that entity. If Event or Condition is listed in this column, the notification code cannot be changed for the alarm condition. When Event is indicated, it is reported as an event only by a report event (REPT EVT) autonomous message. When Condition is indicated, it is not reported and must be retrieved using the RTRV-COND command for that entity.

1.9 If the notification code is CR, MJ, or MN, an alarm autonomous message (REPT ALM) reports changes in the alarm condition for in service (IS) entities. If the entity is out-of-service (OOS-MA or OOS-MT), reporting is suppressed. The RTRV-ALM or RTRV-COND commands are used to retrieve the current state of the alarm.

1.10 If the notification code is NA (Not Alarmed), changes in the alarm condition's state are reported by a REPT EVT autonomous message and are not considered alarmed when active. If the alarm condition is active (standing condition), the RTRV-COND command for that entity reports the condition.

1.11 If the notification code is NR (Not Reported), changes in alarm condition are not reported. However, if the alarm condition is active (standing condition), the RTRV-COND command for that entity reports the condition. Also, even though there is no report when the alarm event occurs, information concerning the event is still retained in the NE. It is reported as an event by a REPT EVT autonomous message. Its notification code cannot be provisioned or changed.

Service-affecting/Nonservice-affecting Behavior

1.12 Service-affecting behavior either is listed as SA (service-affecting) or NSA (nonservice-affecting) for the active side. The condition on the standby side is always NSA. Condition types listed as events are not identified as SA or NSA.

Description

1.13 This column provides a brief text description of the condition.

LED

1.14 This column lists the plug-in unit LED that is lighted by the alarm condition, if applicable. Generally, the LED is on the plug-in unit that is alarmed or on the plug-in unit that terminates the facility or traffic path that is alarmed. These LEDs are controlled by the notification code assigned to the condition.

NOTE *Lamp operation on the COA plug-in unit is not reflected in this column.*

Serial E2A Bit

1.15 This column lists the Serial E2A bit that is provided for TBOS alarm processing remote systems, if applicable. Refer to Appendix C – TBOS Tables in the 1603 SMX Product Information manual for the alarm/status bit map table for TBOS output.

Reference List

1.16 Table C identifies the table reference for each table in this section. The alarms, conditions, and events reported by the 1603 SMX are grouped by the following categories: Equipment, Facilities, Line Group Paths, Drop Group Paths, and Miscellaneous.

Table C. Table References

CATEGORY	TABLE
Equipment	
CCM Unit (CCM101/201)	Table D
CLK Unit (CLK202/203)	Table E
COA Unit (COA60x)	Table F
DMI Unit (DMI102/301)	Table G
HIF Unit (HIF60x/B01/F01)	Table H
LDR Unit (LDR101/201/301)	Table I
LDR Unit (LDR501)	Table J
LIF Unit (LIF201/301)	Table K
LIF Unit (LIF401/404/F01/A01)	Table L
LIF Unit (LIF501/701)	Table M
LIF Unit (LIF601)	Table N
LIF Unit (LIF901)	Table O
LIF Unit (LIFD01)	Table P
LIF Unit (LIFG01)	Table Q
NEP Unit (NEP60x)	Table R
PWR Unit (PWRA01)	Table S
VTG Unit (VTG101/102/301)	Table T
Facilities	
EC1 Facility on LIF201/501/701/D01	Table U
OC3 Facility on HIFB01, OC12 on HIF60x, and OC48 on HIFF01	Table V
OC3 Facility on LIF401/404/F01 and OC12 on LIFA01	Table W
External T1 (DS1) Facility on DMI102/301	Table X
Embedded T1 (DS1) Facility on LIF601	Table Y
T3 Facility on LIF301	Table Z
T3 Facility on LIF501/701/D01	Table AA
SMI Facility (BITS)	Table AC

Table C. Table References (cont)

CATEGORY	TABLE
Line Group Paths	
STS Path on HIFB01/60x/F01	Table AD
VT Path on HIFB01/60x/F01	Table AE
Drop Group Paths	
STS Path on LIF201/301/501/701/D01	Table AF
STS Path on LIF401/404/F01/A01	Table AG
STS Path on LIF901	Table AH
STS Path on LIFG01	Table AI
VT Path on DMI102/301	Table AJ
VT Path on LIF201/501/701/D01	Table AK
VT Path on LIF401/404/F01/A01	Table AL
VT Path on LIF601	Table AM
Miscellaneous	
Adaptation Layer 5 (AAL5)	Table AN
ATM Port	Table AO
ATM Processor	Table AP
Bidirectional Line-Switched Ring (BLSR)	Table AQ
BITS Synchronization Sources	Table AR
CDAC Environmental Alarm Inputs	Table AS
Common Equipment/NE	Table AT
Ports (Craft 1, Craft 2, SE2A, X.25, and PPP)	Table AU
IP Tunnel	Table AV
LLSDCC/LLSMLDCC	Table AW
Local Area Network (LAN)	Table AX
NE Synchronization Sources	Table AY
Network	Table AZ
POS Port	Table BA
Remote NE	Table BB
Synchronous Maintenance Link (SML) Facility	Table BC
Target Identifier Address Resolution Mapping (TADRMAP)	Table BD
USRLAN (LIF901)	Table BE
USRLAN (LIFG01)	Table BF

Table C. Table References

CATEGORY	TABLE
Virtual Channel (VCL)	Table BG
Virtual Path (VPL)	Table BH
X.25 Protocol Stack	Table BI

Table D. Equipment: CCM Unit (CCM101/201)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
BOOT	SA	MJ/MN	Processor is running boot code	ABN (NEP)	53
BUERR	SA	CR/MN	Bus error: Excessive GBI/STS1*/STS1** B2 errors	ALM	20, 21
CONTCOM	NSA	CR/MN	NEP—CCM communication failure	—	—
CONTRDUP	NSA	MJ/MN	Duplex control processor failure	—	—
CTNEQPT	SA	CR/MN	Facility interconnection equipment failure	ALM	20, 21
CLKFAILTOSW	SA	MJ/MN	Clock failed to switch to protection equipment	ALM	20, 21
FAILTOSW	SA	MJ/MN	Failure to switch to protection equipment	—	—
IMPROPRMVL	SA	MJ/MN	Improper removal	—	20, 21
INHDGN	NSA	MN/MN	Diagnostics inhibited	—	—
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
INHSWDX	NSA	MN/MN	Switch to duplex equipment inhibited	ABN (NEP)	53
INT	SA	CR/MN	Internal hardware failure	ALM	20, 21
INVERR	NSA	MJ/MN	Inventory error	ALM	21
MEA	NSA	MJ/MN	Mismatch of equipment or attributes	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
PROGFLT	NSA	MJ/MN	Program storage failure – cannot write to flash memory	ALM	21
PROGVER	NSA	MN/MN	Program version error	ABN (NEP)	53
SYNC	SA	MN/MN	Synchronization failure	ALM	20, 21
SYNCCLK	SA	CR/MN	Synchronization unit clock failure	ALM	20, 21

Table D. Equipment: CCM Unit (CCM101/201) (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AINS	—	Event/ Condition	Unit is in Automatic-In-Service state	—	—
AUTODL	—	Event	Automatic download to CCM in progress	—	—
AUTODLFAIL	—	Event	Automatic download to CCM failed	—	—
AUTORESET-0	—	Event	Automatic reset level 0 (warm restart)	—	—
AUTORESET-1	—	Event	Automatic reset level 1 (cold restart)	—	—
EQUIP	—	Event	CCM is equipped	—	—
FRCDSW	—	Event	Forced equipment switch	—	—
MANRESET-0	—	Event	Manual reset level 0 (warm restart)	—	—
MANRESET-1	—	Event	Manual reset level 1 (cold restart)	—	—
MANRESET-2	—	Event	Manual reset level 2 (download)	—	—
MANSW	—	Event	Manual switch	—	—
UNEQUIP	—	Event	CCM is unequipped	—	—
UNASSIGN	—	Event	CCM is unassigned	—	—
WTRREVERT	—	Event	Wait to restore time out (revert)	—	—
ACT	—	Condition	Unit is active	—	—
STBY	—	Condition	Unit is in standby	—	—
SWDL	—	Condition	Software download in progress—automatic or manual	—	—
CLKSELA	—	Condition	Clock A is selected clock being used by CCM	—	—
CLKSELB	—	Condition	Clock B is selected clock being used by CCM	—	—

Table E. Equipment: CLK Unit (CLK202/203)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
CONTCOM	NSA	MN/MN	NEP-CLK communication failure	ALM	16
FAILTOSW	SA	MJ/MN	Failure to switch to protection equipment	—	15
IMPROPRMVL	SA	MJ/MN	Improper removal	—	15, 16
INHDGN	NSA	MN/MN	Diagnostics inhibited	—	—
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
INHSWDX	NSA	MN/MN	Switch to duplex equipment inhibited	ABN (NEP)	53
INT	SA	CR/MN	Internal hardware fault	ALM	15, 16
INVERR	NSA	MN/MN	Inventory error	ALM	16
MEA	NSA	MN/MN	Mismatch of equipment or attributes	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
PLLEOR	NSA	MN/MN	Phase Locked Loop (PLL) at end of range	ALM	16
SYNCCLK	NSA	MN/MN	Synchronization unit clock failure	ALM	16
AINS	—	Event/ Condition	Unit is in Automatic-In-Service state	—	—
AUTORESET	—	Event	Automatic reset	—	—
AUTOSW	—	Event	Automatic equipment switch	—	—
EQUIP	—	Event	Clock is equipped	—	—
MANSW	—	Event	Manual equipment switch	—	—
UNASSIGN	—	Event	Clock is unassigned	—	—
UNEQUIP	—	Event	Clock is unequipped	—	—
ACT	—	Condition	Unit is active	—	—
STBY	—	Condition	Unit is in standby	—	—

Table F. Equipment: COA Unit (COA60x)

ALARM CONDITION	SRVCE-AFFCTG (Active)	Default NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
BKUPMEMP	NSA	MN	EEPROM failure	ALM	18
CONTCOM	NSA	MN	Control communication failure	ALM	19
IMPROPRMVL	NSA	MJ	Improper removal	—	19
INHDGN	NSA	MN	Inhibit automatic/periodic diagnostics	—	—
INT	NSA	MN	Internal hardware failure	ALM	19
INVERR	NSA	MN	Inventory error	—	19
MEA	NSA	MN	Mismatch of equipment or attributes	—	—
MEMCHK	NSA	MN	Memory checksum error	—	18
MEMDIF	NSA	MN	Mismatch between working and primary databases	—	18
MEMDIFTRAN	NSA	MN	Database mismatch due to translation	—	18
MEMVER	NSA	MN	Version mismatch between working and primary databases	—	18
MTCE	NSA	MN	Removed from service for maintenance	ABN (NEP)	53
PROGFLT	NSA	MN	Program storage failure–cannot write to flash memory	ALM	19
AINS	—	Event/ Condition	Unit is in Automatic-In-Service state	—	—
AUTORESET	—	Event	Automatic reset	—	—
DBCONVERR	—	Event	Database conversion error	—	—
EQUIP	—	Event	COA is equipped	—	—
UNEQUIP	—	Event	COA is unequipped	—	—

Table G. Equipment: DMI Unit (DMI102/301)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
BOOT	SA	MJ/MN	Processor is running boot code	ABN (NEP)	53
BUERR	SA	CR/MN	Bus Error: Excessive STS1* B2 errors	ALM	24, 27
CONTBUS	NSA	CR/MN	Control bus error	ALM	27
CONTCOM	NSA	CR/MN	NEP-DMI link failure	—	—
CONTEQPT	SA	CR/MN	Control equipment failure	ALM	24, 27
CONTRDUP	NSA	MJ/MN	Control duplex processor failure	—	—
CTNEQPT	SA	CR/MN	Facility interconnection equipment failure	ALM	24, 27
FAILTOSW	SA	MJ/MN	Failure to switch to protection equipment	—	36
IMPROPRMVL	SA	MJ/MN	Improper removal	—	24, 27
INHDGN	NSA	MN/MN	Diagnostics inhibited	—	—
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
INHSWDX	NSA	MN/MN	Switch to duplex equipment inhibited	ABN (NEP)	42 & 53
INT	SA	CR/MN	Internal hardware failure	ALM	24, 27
INVERR	NSA	MJ/MN	Inventory error	ALM	27
MEA	NSA	MJ/MN	Mismatch of equipment or attributes	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
PROGFLT	NSA	MJ/MN	Program storage failure—cannot write to flash memory	ALM	27
PROGVER	NSA	MN/MN	Program version error	ABN (NEP)	53
SYNCCLK	SA	CR/MN	Synchronization unit clock failure	ALM	24, 27
AINS	—	Event/ Condition	Unit is in Automatic In-Service state	—	—
AUTODL	—	Event	Automatic download in progress	—	—
AUTODLFAIL	—	Event	Automatic download failed	—	—
AUTORESET-0	—	Event	Automatic reset level 0 (warm restart)	—	—
AUTORESET-1	—	Event	Automatic reset level 1 (cold restart)	—	—
EQUIP	—	Event	DMI is equipped	—	—
FRCDSW	—	Event	Forced switch	—	—
MANRESET-0	—	Event	Manual reset level 0 (warm restart)	—	—

Table G. Equipment: DMI Unit (DMI102/301)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
MANRESET-1	—	Event	Manual reset level 1 (cold restart)	—	—
MANRESET-2	—	Event	Manual reset level 2 (download)	—	—
MANSW	—	Event	Manual equipment switch	—	—
UNASSIGN	—	Event	DMI is unassigned	—	—
UNEQUIP	—	Event	DMI is unequipped	—	—
WTRREVERT	—	Event	Wait to restore time out (revert)	—	—
ACT	—	Condition	Unit is active	—	—
STBY	—	Condition	Unit is in standby	—	—
SWDL	—	Condition	Software download in progress – automatic or manual	—	—
CCMCLKSELA	—	Condition	CCM Clock A is selected clock being used by DMI	—	—
CCMCLKSELB	—	Condition	CCM Clock B is selected clock being used by DMI	—	—

Table H. Equipment: HIF Unit (HIF60x/70x/B01COx/F01/HOx/Jxx)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
BOOT	SA	MJ/MN	Processor is running boot code	ABN (NEP)	53
BUERR	SA	CR/MN	Bus error: Excessive GBI B2 errors	ALM	22, 25 [1] 23, 26 [2]
CONTBUS	SA	CR/MN	Control bus error	ALM	22, 25 [1] 23, 26 [2]
CONTCOM	NSA	CR/MN	NEP-HIF link failure	—	—
CONTEQPT	SA	CR/MN	Control equipment failure	ALM	22, 25 [1] 23, 26 [2]
CONTRDUP	NSA	MJ/MN	Duplex control processor failure	—	—
CTNEQPT	SA	CR/MN	Facility interconnection equipment failure	ALM	22, 25 [1] 23, 26 [2]
HITEMP	NSA	MN/MN	Laser high temperature	ALM	25 [1] 26 [2]
IMPROPRMVL	SA	MJ/MN	Improper removal	—	22, 25 [1] 23, 26 [2]
INHDGN	NSA	MN/MN	Diagnostic inhibited	—	—

Table H. Equipment: HIF Unit (HIF60x/70x/B01COx/F01/HOx/Jxx) (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
INT	SA	CR/MN	Internal hardware failure	ALM	22, 25 [1] 23, 26 [2]
INVERR	NSA	MJ/MN	Inventory error	ALM	25 [1] 26 [2]
LBCL	NSA	MN/MN	Laser bias threshold failure	ALM	25 [1] 26 [2]
LOTEMP	NSA	MN/MN	Laser low temperature	ALM	25 [1] 26 [2]
LPT	NSA	MN/MN	Low laser power (transmitter)	ALM	25 [1] 26 [2]
MEA	NSA	MJ/MN	Mismatch of equipment or attributes	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
PROGFLT	NSA	MJ/MN	Program storage failure – cannot write to flash memory	ALM	25 [1] 26 [2]
PROGVER	NSA	MN/MN	Software program version error	ABN (NEP)	53
SYNC	NSA	MN/MN	Synchronization failure	ALM	25 [1] 26 [2]
SYNCCLK	SA	CR/MN	Synchronization unit clock failure	ALM	22, 25 [1] 23, 26 [2]
AINS	—	Event/ Condition	Unit is in Automatic In-Service state	—	—
AUTODL	—	Event	Automatic download to HIF in progress	—	—
AUTODLFAIL	—	Event	Automatic download to HIF failed	—	—
AUTORESET-0	—	Event	Automatic reset level 0 (warm restart)	—	—
AUTORESET-1	—	Event	Automatic reset level 1 (cold restart)	—	—
EQUIP	—	Event	HIF equipment is equipped	—	—
MANRESET-0	—	Event	Manual reset level 0 (warm restart)	—	—
MANRESET-1	—	Event	Manual reset level 1 (cold restart)	—	—
MANRESET-2	—	Event	Manual reset level 2 (download)	—	—
UNASSIGN	—	Event	HIF is unassigned	—	—
UNEQUIP	—	Event	HIF unit is unequipped	—	—
ACT	—	Condition	Unit is active	—	—
STBY	—	Condition	Unit is in standby	—	—
SWDL	—	Condition	Software download in progress – automatic or manual	—	—

Table H. Equipment: HIF Unit (HIF60x/70x/B01COx/F01/HOx/Jxx)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
CCMCLKSELA	—	Condition	CCM Clock A is selected clock being used by HIF	—	—
CCMCLKSELB	—	Condition	CCM Clock B is selected clock being used by HIF	—	—
[1] *Line Group 1.*					
[2] *Line Group 2.*					

Table I. Equipment: LDR Unit (LDR101/201/301)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
CONTCOM	SA	CR/MN	Active LDR – LIF communication failure	ALM	24, 27
CONTEQPT	SA	MJ/MN	Control equipment failure	ALM	24, 27
CTNEQPT*	SA	CR/MN	Bipolar Data Interface (BDI) failure	ALM	24, 27
FAILTOSW*	SA	MJ/MN	Failure to switch to protection equipment	—	36
IMPROPRMVL	SA	MJ/MN	Improper removal	—	24, 27
INHDGN	NSA	MN/MN	Inhibit automatic/periodic diagnostics	—	—
INHPMREPT	NSA	NR/NR	Inhibit all scheduled PM reports	—	—
INHSWDX*	NSA	MN/MN	Switch to duplex equipment inhibited	ABN (NEP)	42 & 53
INT	SA	CR/MN	Internal hardware failure	ALM	24, 27
INVERR	NSA	MJ/MN	Inventory error	ALM	27
MEA	NSA	MJ/MN	Mismatch of equipment or attributes	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
TRMT	SA	CR/MN	Transmitter failure	ALM	24, 27
AINS	—	Event/ Condition	Unit is in Automatic In-Service state	—	—
AUTORESET	—	Event	Automatic reset	—	—
EQUIP	—	Event	LDR is equipped	—	—
FRCDSW*	—	Event	Forced equipment switch	—	—
MANSW*	—	Event	Manual equipment switch	—	—
UNASSIGN	—	Event	LDR is unassigned	—	—

Table I. Equipment: LDR Unit (LDR101/201/301) (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
UNEQUIP	—	Event	LDR is unequipped	—	—
WTRREVERT*	—	Event	Wait to restore timeout (revert)	—	—
ACT	—	Condition	Unit is active	—	—
STBY	—	Condition	Unit is in standby	—	—
* *This alarm is not applicable if parent LIF is LIF20x or LIF30x.*					

Table J. Equipment: LDR Unit (LDR501)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
CONTCOM	SA	CR	Active LDR – LIF SLI failure	ALM	24, 27
CONTEQPT	SA	MJ	Control equipment failure	ALM	24, 27
CTNEQPT	SA	MJ	Active or standby LIF – LDR Bipolar Data Interface (BDI) test	ALM	24, 27
FAILTOSW	SA	MJ	Failure to switch to protection equipment	—	36
IMPROPRMVL	SA	MJ	Improper removal	—	24, 27
INHDGN	NSA	MN	Inhibit diagnostics	—	—
INHPMREPT	NSA	NR	Inhibit PM reports	—	—
INHSWPR	NSA	MN	Inhibit switch to protection	ABN (NEP)	42 & 53
INHSWWKG	NSA	MN	Inhibit switch to working	ABN (NEP)	42 & 53
INT	SA	CR	LDR alarm	ALM	24, 27
INVERR	NSA	MJ	Inventory error	ALM	24, 27
MEA	NSA	MJ	Mismatch of cards	—	—
MTCE	NSA	MN	Removed from service for maintenance	ABN (NEP)	53
PROTNA	NSA	MN	Protection not available	—	—
AINS	—	Event/ Condition	Unit is in Automatic In-Service state	—	—
AUTORESET	—	Event	Automatic reset	—	—
EQUIP	—	Event	LDR is equipped	—	—
FRCDWKSWBK	—	Event	Forced working switch back	—	—
FRCDWKSWPR	—	Event	Forced working switch to protection	—	—

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
MANWKSWBK	—	Event	Manual working switch back	—	—
MANWKSWPR	—	Event	Manual working switch to protection	—	—
UNASSIGN	—	Event	LDR is unassigned	—	—
UNEQUIP	—	Event	LDR is unequipped	—	—
WKSWBK	—	Event	Working switch back	—	—
WKSWPR	—	Event	Working switch to protection	—	—
WTRREVERT	—	Event	Wait to restore timeout (revert)	—	—
ACT	—	Condition	Unit is active	—	—
STBY	—	Condition	Unit is in standby	—	—

Table K. Equipment: LIF Unit (LIF201/301)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
BOOT	SA	MJ/MN	Processor is running boot code	ABN (NEP)	53
BUERR	SA	CR/MN	Bus error: Excessive STS1** B2 errors	ALM	24, 27
CNTBUS	NSA	CR/MN	Control bus failure	ALM	27
CONTBUS	SA	CR/MN	Control bus error	ALM	24, 27
CONTCOM	NSA	CR/MN	Control communication failure	—	—
CONTEQPT	SA	CR/MN	Control equipment failure	ALM	24, 27
CONTRDUP	NSA	MJ/MN	Duplex control processor failure	—	—
CTNEQPT	SA	CR/MN	Facility interconnection equipment failure	ALM	24, 27
FAILTOSW	SA	MJ/MN	Failure to switch to protection equipment	—	36
IMPROPRMVL	SA	MJ/MN	Improper removal	—	24, 27
INHDGN	NSA	MN/MN	Diagnostics inhibited	—	—
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
INHSWDX	NSA	MN/MN	Switch to duplex equipment inhibited	ABN (NEP)	42 & 53
INT	SA	CR/MN	Internal hardware failure	ALM	24, 27
INVERR	NSA	MJ/MN	Inventory error	ALM	27
MEA	NSA	MJ/MN	Mismatch of equipment or attributes	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53

Table K. Equipment: LIF Unit (LIF201/301) (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PROGFLT	NSA	MJ/MN	Program storage failure – cannot write to flash memory	ALM	27
PROGVER	NSA	MN/MN	Program version error	ABN (NEP)	53
SYNCCLK	SA	CR/MN	Synchronization unit clock failure	ALM	24, 27
AINS	—	Event/ Condition	Unit is in Automatic In-Service state	—	—
AUTODL	—	Event	Automatic download to LIF in progress	—	—
AUTODLFAIL	—	Event	Automatic download to LIF failed	—	—
AUTORESET-0	—	Event	Automatic reset level 0 (warm restart)	—	—
AUTORESET-1	—	Event	Automatic reset level 1 (cold restart)	—	—
EQUIP	—	Event	LIF is equipped	—	—
FRCDSW	—	Event	Forced equipment switch	—	—
MANRESET-0	—	Event	Manual reset level 0 (warm restart)	—	—
MANRESET-1	—	Event	Manual reset level 1 (cold restart)	—	—
MANRESET-2	—	Event	Manual reset level 2 (download restart)	—	—
MANSW	—	Event	Manual equipment switch	—	—
UNASSIGN	—	Event	LIF is unassigned	—	—
UNEQUIP	—	Event	LIF is unequipped	—	—
WTRREVERT	—	Event	Wait to restore timeout (revert)	—	—
ACT	—	Condition	Unit is active	—	—
STBY	—	Condition	Unit is in standby	—	—
SWDL	—	Condition	Software download in progress – automatic or manual	—	—
CCMCLKSELA	—	Condition	CCM Clock A is selected clock being used by LIF	—	—
CCMCLKSELB	—	Condition	CCM Clock B is selected clock being used by LIF	—	—

Table L. Equipment: LIF Unit (LIF401/404/F01/A01)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [3]	DESCRIPTION	LED	SERIAL E2A BIT
BOOT	SA	MJ/MN	Processor is running boot code	ABN (NEP)	53
BUERR	SA	CR/MN	Bus error: STS1* B2 excessive errors	ALM	24, 27
CONTBUS	SA	CR/MN	Control bus error	ALM	24, 27
CONTCOM	NSA	CR/MN	Control communication failure	—	—
CONTEQPT	SA	CR/MN	Control equipment failure	ALM	24, 27
CONTRDUP	NSA	MJ/MN	Duplex control processor failure	—	—
CTNEQPT	SA	CR/MN	Facility interconnection equipment failure	ALM	24, 27
HITEMP	NSA	MN/MN	Laser high temperature	ALM	27
IMPROPRMVL	SA	MJ/MN	Improper removal	—	24, 27
INHDGN	NSA	MN/MN	Diagnostics inhibited	—	—
INT	SA	CR/MN	Internal hardware failure	ALM	24, 27
INVERR	NSA	MJ/MN	Inventory error	ALM	27
LBCL	NSA	MN/MN	Laser bias threshold failure	ALM	27
LOTEMP	NSA	MN/MN	Laser low temperature	ALM	27
LPT	NSA	MN/MN	Low laser power (transmitter)	ALM	27
MEA	NSA	MJ/MN	Mismatch of equipment or attributes	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
PROGFLT	NSA	MJ/MN	Program storage failure – cannot write to flash memory	ALM	27
PROGVER	NSA	MN/MN	Software program version error	ABN (NEP)	53
PROTNA	NSA	MJ/MN	Protection Not Available	—	—
SYNC	NSA	MN/MN	Synchronization failure	ALM	27
SYNCCLK	SA	CR/MN	Synchronization unit clock failure	ALM	24, 27
AINS	—	Event/ Condition	Unit is in Automatic In-Service state	—	—
AUTODL	—	Event	Automatic download to LIF in progress	—	—
AUTODLFAIL	—	Event	Automatic download to LIF failed	—	—
AUTORESET-0	—	Event	Automatic reset level 0 (warm restart)	—	—
AUTORESET-1	—	Event	Automatic reset level 1 (cold restart)	—	—
EQUIP	—	Event	LIF is equipped	—	—

Table L. Equipment: LIF Unit (LIF401/404/F01/A01)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [3]	DESCRIPTION	LED	SERIAL E2A BIT
MANRESET-0	—	Event	Manual reset level 0 (warm restart)	—	—
MANRESET-1	—	Event	Manual reset level 1 (cold restart)	—	—
MANRESET-2	—	Event	Manual reset level 2 (download restart)	—	—
UNASSIGN	—	Event	LIF is unassigned	—	—
UNEQUIP	—	Event	LIF is unequipped	—	—
ACT	—	Condition	Unit is active	—	—
STBY	—	Condition	Unit is in standby	—	—
SWDL	—	Condition	Software download in progress – automatic or manual	—	—
CCMCLKSELA	—	Condition	CCM Clock A is selected clock being used by LIF unit	—	—
CCMCLKSELB	—	Condition	CCM Clock B is selected clock being used by LIF unit	—	—
[3] *Default setting for DUPLEX provisioning shown in table. When provisioned SIMPLEX, the ACT value is used as the default for both A & B sides.*					

Table M. Equipment: LIF Unit (LIF501/701)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
BOOT	SA	MJ/MN	Processor is running boot code	ABN (NEP)	53
BUERR	SA	CR/MN	Bus Error: Excessive STS1* B2 errors	ALM	24, 27
CNTBUS	NSA	CR/MN	Control bus failure	ALM	27
CONTBUS	SA	CR/MN	Control bus error	ALM	24, 27
CONTCOM	NSA	CR/MN	Control communication failure	—	—
CONTEQPT	SA	CR/MN	Control equipment failure	ALM	24, 27
CONTRDUP	NSA	MJ/MN	Duplex control processor failure	—	—
CTNEQPT	SA	CR/MN	Facility interconnection equipment failure	ALM	24, 27
FAILTOSW	SA	MJ/MN	Failure to switch to protection equipment	—	36
IMPROPRMVL	SA	MJ/MN	Improper removal	—	24, 27
INHDGN	NSA	MN/MN	Diagnostics inhibited	—	—

Table M. Equipment: LIF Unit (LIF501/701) (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
INHSWDX	NSA	MN/MN	Switch to duplex equipment inhibited	ABN (NEP)	42 & 53
INT	SA	CR/MN	Internal hardware failure	ALM	24, 27
INVERR	NSA	MJ/MN	Inventory error	ALM	27
MEA	NSA	MJ/MN	Mismatch of equipment or attributes	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
PROGFLT	NSA	MJ/MN	Program storage failure – cannot write to flash memory	ALM	27
PROGVER	NSA	MN/MN	Software program version error	ABN (NEP)	53
SYNCCLK	SA	CR/MN	Synchronization unit clock failure	ALM	24, 27
SYNCSEL	NSA	MN/MN	Synchronization output already in use	—	—
AINS	—	Event/ Condition	Unit is in Automatic In-Service state	—	—
AUTODL	—	Event	Automatic download to LIF in progress	—	—
AUTODLFAIL	—	Event	Automatic download to LIF failed	—	—
AUTORESET-0	—	Event	Automatic reset level 0 (warm restart)	—	—
AUTORESET-1	—	Event	Automatic reset level 1 (cold restart)	—	—
EQUIP	—	Event	LIF is equipped	—	—
FRCDSW	—	Event	Forced equipment switch	—	—
MANRESET-0	—	Event	Manual reset level 0 (warm restart)	—	—
MANRESET-1	—	Event	Manual reset level 1 (cold restart)	—	—
MANRESET-2	—	Event	Manual reset level 2 (download restart)	—	—
MANSW	—	Event	Manual equipment switch	—	—
UNASSIGN	—	Event	LIF is unassigned	—	—
UNEQUIP	—	Event	LIF is unequipped	—	—
WTRREVERT	—	Event	Wait to restore timeout (revert)	—	—
ACT	—	Condition	Unit is active	—	—
STBY	—	Condition	Unit is in standby	—	—
SWDL	—	Condition	Software download in progress – automatic or manual	—	—

Table M. Equipment: LIF Unit (LIF501/701)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
CCMCLKSELA	—	Condition	CCM Clock A is selected clock being used by LIF	—	—
CCMCLKSELB	—	Condition	CCM Clock B is selected clock being used by LIF	—	—

Table N. Equipment: LIF Unit (LIF601)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
BOOT	SA	MJ/MN	Processor is running boot code	ABN (NEP)	53
BUERR	SA	CR/MN	Bus error: Excessive STS1* B2 errors	ALM	24, 27
CONTBUS	SA	CR/MN	Control bus error	ALM	24, 27
CONTCOM	NSA	CR/MN	Control communication failure	—	—
CONTEQPT	SA	CR/MN	Control equipment failure	ALM	24, 27
CONTRDUP	NSA	MJ/MN	Duplex control processor failure	—	—
CNTBUS	NSA	CR/MN	Control bus failure	ALM	27
CTNEQPT	SA	CR/MN	Facility interconnection equipment failure	ALM	24, 27
FAILTOSW	SA	MJ/MN	Failure to switch to protection equipment	—	36
IMPROPRMVL	SA	MJ/MN	Improper removal	—	24, 27
INHDGN	NSA	MN/MN	Diagnostics inhibited	—	—
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
INHSWDX	NSA	MN/MN	Switch to duplex equipment inhibited	ABN (NEP)	42 & 53
INT	SA	CR/MN	Internal hardware failure	ALM	24, 27
INVERR	NSA	MJ/MN	Inventory error	ALM	27
MEA	NSA	MJ/MN	Mismatch of equipment or attributes	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
PROGFLT	NSA	MJ/MN	Program storage failure – cannot write to flash memory	ALM	27
PROGVER	NSA	MN/MN	Software program version error	ABN (NEP)	53
SYNCCLK	SA	CR/MN	Synchronization unit clock failure	ALM	24, 27

Table N. Equipment: LIF Unit (LIF601) (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
SYNC	NSA	MN/MN	Synchronization failure	ALM	27
AINS	—	Event/ Condition	Unit is in Automatic In-Service state	—	—
AUTODL	—	Event	Automatic download to LIF in progress	—	—
AUTODLFAIL	—	Event	Automatic download to LIF failed	—	—
AUTORESET-0	—	Event	Automatic reset level 0 (warm restart)	—	—
AUTORESET-1	—	Event	Automatic reset level 1 (cold restart)	—	—
EQUIP	—	Event	LIF is equipped	—	—
FRCDSW	—	Event	Forced switch	—	—
MANRESET-0	—	Event	Manual reset level 0 (warm restart)	—	—
MANRESET-1	—	Event	Manual reset level 1 (cold restart)	—	—
MANRESET-2	—	Event	Manual reset level 2 (download restart)	—	—
MANSW	—	Event	Manual switch	—	—
UNASSIGN	—	Event	LIF is unassigned	—	—
UNEQUIP	—	Event	LIF is unequipped	—	—
WTRREVERT	—	Event	Wait to restore timeout (revert)	—	—
ACT	—	Condition	Unit is active	—	—
STBY	—	Condition	Unit is in standby	—	—
SWDL	—	Condition	Software download in progress – automatic or manual	—	—
CCMCLKSELA	—	Condition	CCM Clock A is selected clock being used by LIF	—	—
CCMCLKSELB	—	Condition	CCM Clock B is selected clock being used by LIF	—	—

Table O. Equipment: LIF Unit (LIF901)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
BOOT	SA	MJ/MN	Processor is running boot code	ABN (NEP)	53
BUERR	SA	CR/MN	Bus error: Excessive STS1* B2 errors	ALM	24
CONTBUS	SA	CR/MN	Control bus error	ALM	24
CONTCOM	NSA	CR/MN	NEP-LIF link failure	—	—
CONTEQPT	SA	CR/MN	Switch test failure	ALM	24
CTNEQPT	SA	CR/MN	Facility interconnection equipment failure	ALM	24
FWCONTCOM	NSA	CR/MN	Loss of communication to ethernet	—	—
FWMJVER	NSA	MJ/MN	Firmware major version error	ABN (LED)	—
FWMNVER	NSA	MJ/MN	Firmware minor version error	—	—
FWPROGFLT	NSA	MJ/MN	Firmware program error	—	—
IMPROPRMVL	SA	MJ/MN	Improper removal	—	24
INHDGN	NSA	MN/MN	Diagnostics inhibited	—	—
INT	SA	CR/MN	Internal hardware failure	ALM	24
INVERR	NSA	MJ/MN	Inventory error	ALM	27
MEA	NSA	MJ/MN	Mismatch of cards	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
PROGFLT	NSA	MJ/MN	Program storage failure – cannot write to flash memory	ALM	27
PROGVER	NSA	MN/MN	Software program version error	ABN (NEP)	53
SYNC	NSA	MN/MN	Synchronization failure	ALM	27
SYNCCLK	SA	CR/MN	Synchronization unit clock failure	ALM	24
AINS	—	Event/ Condition	Unit is in Automatic-In-Service state	—	—
AUTODL	—	Event	Automatic download to LIF in progress	—	—
AUTODLFAIL	—	Event	Automatic download to LIF failed	—	—
AUTORESET-0	—	Event	Automatic reset level 0 (warm restart)	—	—
AUTORESET-1	—	Event	Automatic reset level 1 (cold restart)	—	—
EQUIP	—	Event	LIF is equipped	—	—

Table O. Equipment: LIF Unit (LIF901)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
FWAUTODL	—	Event	Firmware automatic download in progress	—	—
FWAUTODLFAIL	—	Event	Firmware automatic download failure	—	—
FWAUTORESET	—	Event	Firmware automatic reset	—	—
MANRESET-0	—	Event	Manual reset level 0 (warm restart)	—	—
MANRESET-1	—	Event	Manual reset level 1 (cold restart)	—	—
MANRESET-2	—	Event	Manual reset level 2 (download)	—	—
UNEQUIP	—	Event	LIF is unequipped	—	—
ACT	—	Condition	Unit is active	—	—
SWDL	—	Condition	Software download in progress – automatic or manual	—	—
CCMCLKSELA	—	Condition	CCM Clock A is selected clock being used by LIF	—	—
CCMCLKSELB	—	Condition	CCM Clock B is selected clock being used by LIF	—	—
FWDL	—	Condition	Firmware download in progress	—	—

Table P. Equipment: LIF Unit (LIFD01)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE	DESCRIPTION	LED	SERIAL E2A BIT
BOOT	SA	MJ/MN	Processor is running boot code	ABN (NEP)	53
BUERR	SA	CR/MN	Bus error: Excessive STS1* B2 errors	ALM	24, 27
CNTBUS	NSA	CR/MN	Control bus failure	ALM	27
CONTBUS	SA	CR/MN	Control bus error	ALM	24, 27
CONTCOM	NSA	CR/MN	NEP-LIF link failure	—	—
CONTEQPT	SA	CR/MN	Switch test failure	ALM	24, 27
CONTRDUP	NSA	MJ/MN	Active/standby LIF link failure	—	—
CTNEQPT	SA	CR/MN	Facility interconnection equipment failure	ALM	24, 27
FAILTOSW	SA	MJ/MN	Failure to Switch	—	36
IMPROPRMVL	SA	MJ/MN	Improper removal	—	24, 27
INHDGN	NSA	MN/MN	Diagnostics inhibited	—	—

Table P. Equipment: LIF Unit (LIFD01) (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE	DESCRIPTION	LED	SERIAL E2A BIT
INHPMREPT	NSA	NR/NR	PM report inhibited	—	—
INHSWDX	NSA	MN/MN	Switch inhibited	ABN (NEP)	42 & 53
INT	SA	CR/MN	Redundant LIF fails	ALM	24, 27
INVERR	NSA	MJ/MN	Inventory error	ALM	27
MEA	NSA	MJ/MN	Mismatch of cards	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
PROGFLT	NSA	MJ/MN	Program storage failure – cannot write to flash memory	ALM	27
PROGVER	NSA	MN/MN	Software program version error	ABN (NEP)	53
SYNC	NSA	MN/MN	Synchronization failure	ALM	27
SYNCCLK	SA	CR/MN	Synchronization unit clock failure	ALM	24, 27
AINS	—	Event/ Condition	Unit is in Automatic In-Service state	—	—
AUTODL	—	Event	Automatic download to LIF in progress	—	—
AUTODLFAIL	—	Event	Automatic download to LIF failed	—	—
AUTORESET-0	—	Event	Automatic reset level 0 (warm restart)	—	—
AUTORESET-1	—	Event	Automatic reset level 1 (cold restart)	—	—
EQUIP	—	Event	LIF is equipped	—	—
FRCDSW	—	Event	Forced switch	—	—
MANRESET-0	—	Event	Manual reset level 0 (warm restart)	—	—
MANRESET-1	—	Event	Manual reset level 1 (cold restart)	—	—
MANRESET-2	—	Event	Manual reset level 2 (download)	—	—
MANSW	—	Event	Manual switch	—	—
UNEQUIP	—	Event	LIF is unequipped	—	—
UNASSIGN	—	Event	LIF is unassigned	—	—
WTRREVERT	—	Event	Wait to restore/revertive time out	—	—
ACT	—	Condition	Unit is active	—	—
STBY	—	Condition	Unit is on standby	—	—
SWDL	—	Condition	Software download in progress – automatic or manual	—	—

Table P. Equipment: LIF Unit (LIFD01)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE	DESCRIPTION	LED	SERIAL E2A BIT
CCMCLKSELA	—	Condition	CCM Clock A is selected clock being used by LIF	—	—
CCMCLKSELB	—	Condition	CCM Clock B is selected clock being used by LIF	—	—

Table Q. Equipment: LIF Unit (LIFG01)

ALARM CONDITION	SRVCE-AFFCTG	DEFAULT NTFCNCDE A/B	DESCRIPTION	LED	SERIAL E2A BIT
BOOT	SA	MJ/MJ	Processor is running boot code	ABN (NEP)	53
BUERR	SA	CR/CR	Bus error: Excessive STS1* B2 errors	ALM	24
CONTBUS	SA	CR/CR	Control bus error	ALM	24
CONTCOM	NSA	CR/CR	NEP-LIF link failure	—	—
CONTEQPT	SA	CR/CR	Switch test failure	ALM	24
CTNEQPT	SA	CR/CR	Facility interconnection equipment failure	ALM	24
IMPROPRMVL	SA	MJ/MJ	Improper removal	—	24
INHDGN	NSA	MN/MN	Diagnostics inhibited	—	—
INT	SA	CR/CR	Internal hardware failure	ALM	24
INVERR	NSA	MJ/MJ	Inventory error	ALM	27
MEA	NSA	MJ/MJ	Mismatch of cards	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
PROGFLT	NSA	MJ/MJ	Program storage failure – cannot write to flash memory	ALM	27
PROGVER	NSA	MN/MN	Software program version error	ABN (NEP)	53
SYNC	NSA	MN/MN	Synchronization failure	ALM	27
SYNCCLK	SA	CR/CR	Synchronization unit clock failure	ALM	24
AINS	—	Event/ Condition	Unit is in Automatic-In-Service state	—	—
AUTODL	—	Event	Automatic download to LIF in progress	—	—
AUTODLFAIL	—	Event	Automatic download to LIF failed	—	—

Table Q. Equipment: LIF Unit (LIFG01)

ALARM CONDITION	SRVCE-AFFCTG	DEFAULT NTFCNCDE A/B	DESCRIPTION	LED	SERIAL E2A BIT
AUTORESET-0	—	Event	Automatic reset level 0 (warm restart)	—	—
AUTORESET-1	—	Event	Automatic reset level 1 (cold restart)	—	—
EQUIP	—	Event	LIF is equipped	—	—
MANRESET-0	—	Event	Manual reset level 0 (warm restart)	—	—
MANRESET-1	—	Event	Manual reset level 1 (cold restart)	—	—
MANRESET-2	—	Event	Manual reset level 2 (download)	—	—
UNEQUIP	—	Event	LIF is unequipped	—	—
ACT	—	Condition	Unit is active	—	—
SWDL	—	Condition	Software download in progress – automatic or manual	—	—
CCMCLKSELA	—	Condition	CCM Clock A is selected clock being used by LIF	—	—
CCMCLKSELB	—	Condition	CCM Clock B is selected clock being used by LIF	—	—

Table R. Equipment: NEP Unit (NEP60x)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE	DESCRIPTION	LED	SERIAL E2A BIT
CONTBUS	NSA	MN	Control bus error	ALM	18
CONTEQPT	NSA	MN	Control equipment failure	ALM	18
INHDGN	NSA	MN	Diagnostics inhibited	—	—
INT	NSA	MJ	Internal hardware failure	ALM	18
INVERR	NSA	MN	Inventory error	ALM	18
MEA	NSA	MN	Mismatch of equipment or attributes	—	—
MTCE	NSA	MN	Removed from service for maintenance	ABN	53
SYNC	NSA	MN	Synchronization failure	ALM	18
SYNCCLK	NSA	MN	Synchronization unit clock failure	ALM	18
AUTORESET-0	—	Event	Automatic reset level 0 (warm restart)	—	—
AUTORESET-1	—	Event	Automatic reset level 1 (cold restart)	—	—
MANRESET-0	—	Event	Manual reset level 0 (warm restart)	—	—
MANRESET-1	—	Event	Manual reset level 1 (cold restart)	—	—

Table R. Equipment: NEP Unit (NEP60x)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE	DESCRIPTION	LED	SERIAL E2A BIT
MANRESET-2	—	Event	Manual reset level 2 (download restart)	—	—
ACT	—	Condition	Unit is active	—	—

Table S. Equipment: PWR Unit (PWRA01)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
CNVT	NSA	MN	Power converter failure	ALM	13
IMPROPRMVL	NSA	MJ	Improper removal	—	13
INT	NSA	MN	Internal hardware failure	ALM	13
INVERR	NSA	MN	Inventory error	ALM	13
MEA	NSA	MN	Mismatch of equipment or attributes	—	—
MTCE	NSA	MN	Removed from service for maintenance	ABN (NEP)	53
AINS	—	Event/ Condition	Unit is in Automatic In-Service state	—	—
EQUIP	—	Event	Unit is equipped	—	—
UNEQUIP	—	Event	Unit is unequipped	—	—

Table T. Equipment: VTG Unit (VTG101/102/301)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
BUERR	SA	MJ	VTG group parity error, VTG bus failure	ALM	24, 27
CONTBUS	SA	MJ	Control bus error	ALM	24, 27
CONTEQPT	SA	MJ	Control equipment failure	ALM	24, 27
FAILTOSW	SA	MJ	Failure to switch to protection equipment	—	36
IMPROPRMVL	SA	MJ	Improper removal	—	24, 27
INHPMREPT	NSA	NR	All scheduled PM reports inhibited	—	—
INHDGN	NSA	MN	Diagnostics inhibited	—	—
INHSWPR	NSA	MN	Switch to protection equipment inhibited	ABN (NEP)	42 & 53
INHSWWKG	NSA	MN	Switch to working equipment inhibited	ABN (NEP)	42 & 53
INT	SA	MJ	Internal hardware failure	ALM	24, 27
INVERR	NSA	MJ	Inventory error	ALM	27
MEA	NSA	MJ	Mismatch of equipment or attributes	—	—
MTCE	NSA	MN	Removed from service for maintenance	ABN (NEP)	53
PROTNA	NSA	MN	Protection not available	—	—
SWEQPT	SA	MJ	Equipment switch	ALM	24, 27
SYNC	SA	MJ	Synchronization failure	ALM	24, 27
SYNCCLK	SA	MJ	Synchronization unit clock failure	ALM	24, 27
AINS	—	Event/ Condition	Unit is in Automatic In-Service state	—	—
EQUIP	—	Event	VTG is equipped	—	—
FRCDWKSWBK	—	Event	Force switch back to working	—	—
FRCDWKSWPR	—	Event	Working equipment forced to switch to protection	—	—
MANWKSWBK	—	Event	Manual switch back to working	—	—
MANWKSWPR	—	Event	Manual switch of working equipment to protection	—	—
UNASSIGN	—	Event	VTG is unassigned	—	—
UNEQUIP	—	Event	VTG is unequipped	—	—
WKSWBK	—	Event	Switch back to working	—	—

Table T. Equipment: VTG Unit (VTG101/102/301)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
WKSWPR	—	Event	Working equipment switched to protection	—	—
WTRREVERT	—	Event	Wait to restore timeout (revert)	—	—
ACT	—	Condition	Unit is active	—	—
STBY	—	Condition	Unit is in standby	—	—

Table U. Facility: EC1 on LIF201/501/701/D01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AISL	SA	NR	Line alarm indication signal detected	SF	30
APSB	SA	MJ	APS byte failure	—	30
BERL-HT	SA	CR	Signal failure bit error rate threshold crossed	SF	30
BERL-LT	SA	MJ	Signal degraded bit error ratio threshold crossed	—	30
INHPMREPT	NSA	NR	All scheduled PM reports inhibited	—	—
LOF	SA	CR	Loss-of-frame	SF	30
LOS	SA	CR	Loss-of-signal	SF	30
MTCE	NSA	MN	Removed from service for maintenance	ABN (NEP)	53
RFI	SA	NR	Far end receiver failure	—	30
SECTRCMF	NSA	MN	Section tracer mismatch	—	—
SYNCLEVINCHG	NSA	NA [1]	Synchronization level input change	—	—
SYNCLEVINFAIL	NSA	MN	Synchronization level input failure	—	—
T-BPV	NSA	NA	Threshold violation for bipolar errors [2]	—	—
T-CVL	NSA	NA	Threshold violation for PM line BIP errors [2] – NE	—	—
T-CVL	NSA	NA	Threshold violation for PM line BIP errors [2] – FE	—	—
T-CVS	NSA	NA	Threshold violation for PM section BIP errors [2]	—	—
T-ESL	NSA	NA	Threshold violation for PM line errored seconds [2] – NE	—	—

Table U. Facility: EC1 on LIF201/501/701/D01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
T-ESL	NSA	NA	Threshold violation for PM line errored seconds [2] – FE	—	—
T-ESS	NSA	NA	Threshold violation for PM section errored seconds [2]	—	—
T-SEFS	NSA	NA	Threshold violation for PM severely errored framing seconds [2]	—	—
T-SESL	NSA	NA	Threshold violation for PM line severely errored seconds [2] – NE	—	—
T-SESL	NSA	NA	Threshold violation for PM line severely errored seconds [2] – FE	—	—
T-SESS	NSA	NA	Threshold violation for PM section severely errored seconds [2]	—	—
T-UASL	NSA	NA	Threshold violation for PM line unavailable seconds [2] – NE	—	—
T-UASL	NSA	NA	Threshold violation for PM line unavailable seconds [2] – FE	—	—
ACTLPBK	—	Event/ Condition	Loopback is active	—	—
AINS	—	Event/ Condition	Automatic In-Service state	—	—
IS-AUTO	—	Event	Automatic OOS-MA to IS	—	—
SECTRCHG	—	Event	Section tracer change	—	—
SYNCLEVIN-n where: n = 0...15	—	Condition	Value of synchronization input level	—	—
SYNCLEVOUT–n where: n = 0...15	—	Condition	Value of synchronization output level	—	—

[1] *The notification code for this condition only can be provisioned as NR or NA.*

[2] *Either 15-minute or 1-day Threshold Crossing Alert (TCA).*

Table V. Facility: OC3 on HIFB01, OC12 on HIF60x, and OC48 on HIFF01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AISL	SA	NR/NR	Line alarm indication signal detected	SF	28, 31 [1] 29, 32 [2]
ALS	SA	MN/MN	Automatic laser shutdown	—	—
APSB	SA	MJ/MN	APS (automatic protection switching) byte failure	—	28, 31 [1] 29, 32 [2]
APSCM	SA	MJ/MN	APS channel match failure	—	28, 31 [1] 29, 32 [2]
APSDFLT [3]	NSA	MJ/MN	Default K byte detected or transmitted	—	—
APSIMPROP [3]	NSA	MJ/MN	Improper APS switch code	—	—
APSINCON [3]	NSA	MJ/MN	Inconsistent APS switch code	—	—
APSMM	SA	MJ/MN	APS mode mismatch	—	28, 31 [1] 29, 32 [2]
APSNODEIDMM [3]	NSA	MJ/MN	Node ID mismatch	—	—
BERL-HT	SA	CR/MN	Signal failure bit error rate threshold crossed	SF	28, 31 [1] 29, 32 [2]
BERL-LT	SA	MJ/MN	Signal degraded bit error ratio threshold crossed	—	28, 31 [1] 29, 32 [2]
FAILTOSW	SA	MJ/MN	Failure to switch to protection equipment	—	34 [1] 35 [2]
FAILTOSW-RING [3]	NSA	MN/MN	Failure to switch ring	—	34 [1] 35 [2]
FEPRLF	SA	MN/MN	Far end protection line failure	—	28, 31 [1] 29, 32 [2]
FRCD	NSA	MN/MN	Forced switch	ABN (NEP)	53
FRCD-RING [3]	NSA	MN/MN	Forced switch ring (working to protection)	ABN (NEP)	53
INHEX-RING [3]	NSA	NR/NR	Inhibit exercise switch ring	—	—
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
LINENA	SA	CR/MN	Line not available	—	28, 31 [1] 29, 32 [2]
LOCKOUT-LOWR [3]	NSA	MN/MN	Lockout switch ring (local NE)	ABN (NEP)	40 [1] 41 [2] 53
LOCKOUT-LPS [3]	NSA	MN/MN	Lockout switch span (entire ring)	ABN (NEP)	40 [1] 41 [2] 53

Table V. Facility: OC3 on HIFB01, OC12 on HIF60x, and OC48 on HIFF01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
LOCKOUTOFPR	NSA	MN/MN	APS lock out of protection	ABN (NEP)	40 [1] 41 [2] 53
LOF	SA	CR/MN	Loss-of-frame	SF	28, 31 [1] 29, 32 [2]
LOS	SA	CR/MN	Loss-of-signal or clock	SF	28, 31 [1] 29, 32 [2]
LPR	NSA	MN/MN	Low laser light (receiver)	—	—
MAN	NSA	MN/MN	Manual switch	ABN (NEP)	53
MAN-RING [3]	NSA	MN/MN	Manual switch ring (working to protection)	ABN (NEP)	53
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
RFI	SA	NR/NR	Far end receiver failure	—	28, 31 [1] 29, 32 [2]
SECTRCMF	NSA	MN/MN	Section tracer mismatch	—	—
SECTRCERR (OC48 only)	NSA	CR/MN	Section tracer error (Rx and Tx trace match)	—	—
SWEX-RING [3]	NSA	MN/MN	Exercise switch ring failure	—	—
SYNCLEVINCHG	NSA	NA/NA[5]	Synchronization message change	—	—
SYNCLEVINFAIL	NSA	MN/MN	Synchronization message failure	—	—
T-CVL	NSA	NA/NA	Threshold violation for line BIP errors [4] – FE	—	—
T-CVL	NSA	NA/NA	Threshold violation for PM line BIP errors [4] – NE	—	—
T-CVS	NSA	NA/NA	Threshold violation for PM section BIP errors [4] – NE	—	—
T-ESL	NSA	NA/NA	Threshold violation for line errored seconds [4] – FE	—	—
T-ESL	NSA	NA/NA	Threshold violation for PM line errored seconds [4] – NE	—	—
T-ESS	NSA	NA/NA	Threshold violation for PM section errored seconds [4] – NE	—	—
T-SEFS	NSA	NA/NA	Threshold violation for PM severely errored framing seconds [4] – NE	—	—

Table V. Facility: OC3 on HIFB01, OC12 on HIF60x, and OC48 on HIFF01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
T-SESL	NSA	NA/NA	Threshold violation for line severely errored seconds [4] – FE	—	—
T-SESL	NSA	NA/NA	Threshold violation for PM line severely errored seconds [4] – NE	—	—
T-SESS	NSA	NA/NA	Threshold violation for PM section severely errored seconds [4] – NE	—	—
T-UASL	NSA	NA/NA	Threshold violation for line unavailable seconds [4] – FE	—	—
T-UASL	NSA	NA/NA	Threshold violation for PM line unavailable seconds [4] – NE	—	—
ACTLPBK	—	Event/ Condition	Loopback is active	—	—
AINS	—	Event/ Condition	Automatic In-Service state	—	—
FRCDWKSWBK	—	Event	Forced switch back to working; near end or far end	—	—
FRCDWKSWPR	—	Event	Forced switch to protection; near end or far end	—	—
FRCDWKSWPR-RING [3]	—	Event	Forced switching to protection	—	—
IS-AUTO	—	Event	Automatic OOS-MA to IS	—	—
LOCKOUTOFPR	—	Event	Lock out of protection; near end or far end	—	—
MANWKSWBK	—	Event	Manual switch back to working; near end or far end	—	—
MANWKSWPR	—	Event	Manual switch from working to protection; near end or far end	—	—
MANWKSWPR-RING [3]	—	Event	Manual switching to protection	—	—
SECTRCHG	—	Event	Section trace change	—	—
SIGDEG	—	Event	Far end: signal degraded	—	—
SIGDEG-RING [3]	—	Event	Signal degraded	—	—
SIGFAIL	—	Event	Far end: signal failure	—	—
SIGFAIL-RING [3]	—	Event	Signal failure	—	—
UNASSIGN	—	Event	Facility is unassigned	—	—
WKSWBK	—	Event	Switch back to working	—	—

Table V. Facility: OC3 on HIFB01, OC12 on HIF60x, and OC48 on HIFF01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
WKSWBK-RING [3]	—	Event	Switch back to working	—	—
WKSWPR	—	Event	Working equipment switched to protection	—	—
WKSWPR-RING [3]	—	Event	Switch to protection	—	—
WTRREVERT	—	Event	Wait to restore timeout (revert)	—	—
WTRREVERT-RING [3]	—	Event	Wait for restore timeout (revert)	—	—
ACT	—	Condition	Facility is active; near end or far end	—	—
BRIDGE [3]	—	Condition	Bridge active	—	—
STBY	—	Condition	Facility is in standby; near end or far end	—	—
K1-xx (rcv) where x = 0..255	—	Condition	Contents of K1 byte	—	—
K1-xx (trmt) where x = 0..255 [3]	—	Condition	Contents of K1 byte	—	—
K2-xx (rcv) where x = 0..255	—	Condition	Contents of K2 byte	—	—
K2-xx (trmt) where x = 0..255 [3]	—	Condition	Contents of K2 byte	—	—
SYNCLEVIN-n where n = 0..15	—	Condition	Synchronization quality level input	—	—
SYNCLEVOUT-n where n = 0..15	—	Condition	Synchronization quality level output	—	—

[1] *Line Group 1.*

[2] *Line Group 2.*

[3] *OC48 BLSR only.*

[4] *Either 15-minute or 1-day Threshold Crossing Alert (TCA).*

[5] *The SYNCLEVINCHG can only be provisioned as NA or NR.*

Table W. Facility: OC3 on LIF401/404/F01 and OC12 on LIFA01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [3]	DESCRIPTION	LED	SERIAL E2A BIT
AISL	SA	NR/NR	Line alarm indication signal detected	SF	30, 33
ALS	SA	MN/MN	Automatic laser shutdown	—	—
APSB	SA	MJ/MN	APS (Automatic Protection Switch) byte failure	—	30, 33
APSCM	SA	MJ/MN	APS channel match failure	—	30, 33
APSMM	SA	MJ/MN	APS mode mismatch	—	30, 33
BERL-HT	SA	CR/MN	Signal failure bit error rate threshold crossed	SF	30, 33
BERL-LT	SA	MJ/MN	Signal degraded bit error ratio threshold crossed	—	30, 33
FAILTOSW	SA	MJ/MN	Failure to switch to protection equipment	—	36
FEPRLF	SA	MN/MN	Far end protection line failure	—	30, 33
FRCD	NSA	MN/MN	Forced switch	ABN (NEP)	53
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
LINENA	SA	CR/MN	Line not available	—	30, 33
LOCKOUTOFPR	NSA	MN/MN	Lock out of protection	ABN (NEP)	42 & 53
LOF	SA	CR/MN	Loss-of-frame	SF	30, 33
LOS	SA	CR/MN	Loss-of-signal	SF	30, 33
LPR	NSA	MN/MN	Low laser light (receiver)	—	—
MAN	NSA	MN/MN	Manual switch	ABN (NEP)	53
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
RFI	SA	NR/NR	Far end receiver failure	—	30, 33
SECTRCMF	NSA	MN/MN	Section tracer mismatch	—	—
SYNCLEVINCHG	NSA	NA/NA [1]	Synchronization message change	—	—
SYNCLEVINFAIL	NSA	MN/MN	Synchronization message failure	—	—
T-CVL	NSA	NA/NA	Threshold violation for PM line BIP errors [2] – NE	—	—
T-CVL	NSA	NA/NA	Threshold violation for line BIP errors [2] – FE	—	—
T-CVS	NSA	NA/NA	Threshold violation for PM section BIP errors [2]	—	—

Table W. Facility: OC3 on LIF401/404/F01 and OC12 on LIFA01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [3]	DESCRIPTION	LED	SERIAL E2A BIT
T-ESL	NSA	NA/NA	Threshold violation for PM line errored seconds [2] – NE	—	—
T-ESL	NSA	NA/NA	Threshold violation for line errored seconds [2] – FE	—	—
T-ESS	NSA	NA/NA	Threshold violation for PM section errored seconds [2]	—	—
T-SEFS	NSA	NA/NA	Threshold violation for PM severely errored framing seconds [2]	—	—
T-SESL	NSA	NA/NA	Threshold violation for PM line severely errored seconds [2] – NE	—	—
T-SESL	NSA	NA/NA	Threshold violation for line severely errored seconds [2] – FE	—	—
T-SESS	NSA	NA/NA	Threshold violation for PM section severely errored seconds [2]	—	—
T-UASL	NSA	NA/NA	Threshold violation for line unavailable seconds [2] – NE	—	—
T-UASL	NSA	NA/NA	Threshold violation for PM line unavailable seconds [2] – FE	—	—
ACTLPBK	—	Event/ Condition	Loopback is active	—	—
AINS	—	Event/ Condition	Automatic In-Service state	—	—
FRCDWKSWBK	—	Event	Forced switch back to working; near end or far end	—	—
FRCDWKSWPR	—	Event	Working equipment forced to switch to protection; near end or far end	—	—
IS-AUTO	—	Event	Automatic OOS-MA to IS	—	—
LOCKOUTOFPR	—	Event	Lock out of protection; near end or far end	—	—
MANWKSWBK	—	Event	Manual switch back to working; near end or far end	—	—
MANWKSWPR	—	Event	Manual switch of working equipment to protection; near end or far end	—	—
SECTRCHG	—	Event	Section tracer changed	—	—
SIGFAIL	—	Event	Far end: signal failure	—	—
SIGDEG	—	Event	Far end: signal degraded	—	—
UNASSIGN	—	Event	Facility is unassigned	—	—

Table W. Facility: OC3 on LIF401/404/F01 and OC12 on LIFA01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [3]	DESCRIPTION	LED	SERIAL E2A BIT
WKSWBK	—	Event	Switch back to working	—	—
WKSWPR	—	Event	Working equipment switched to protection	—	—
WTRREVERT	—	Event	Wait to restore timeout (revert) – NE and FE	—	—
ACT	—	Condition	Facility is active; near end or far end	—	—
K1-xx where xx = 0...255	—	Condition	Contents of K1 byte	—	—
K2-xx where xx = 0...255	—	Condition	Contents of K2 byte	—	—
STBY	—	Condition	Facility is in standby; near end or far end	—	—
SYNCLEVIN-n where: n = 0...15	—	Condition	Synchronization quality level input value	—	—
SYNCLEVOUT-n where: n = 0...15	—	Condition	Synchronization quality level output value	—	—

[1] *The SYNCLEVINCHG event can only be provisioned as NA or NR.*

[2] *Either 15-minute or a 1-day Threshold Crossing Alert (TCA).*

[3] *Default setting for DUPLEX provisioning shown in table. When the parent equipment is provisioned SIMPLEX, the ACT value is used as the default for both A & B sides.*

Table X. Facility: External T1 (DS1) on DMI102/301

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AIS	SA	NR	Alarm indication signal detected – RCV (NE)	SF	30
AIS (VTG301)	SA	NR	Alarm indication signal detected – TRMT (FE)	—	30
BERL-HT	SA	MJ	Signal failure bit error rate threshold crossed	SF	30
DS1ISD (VTG301)	SA	NR	Rx idle	—	30
INHLPBK-ESFLINE (VTG301)	NSA	NR	Inhibit loopback	—	—
INHLPBK-INBAND-RX	NSA	NR	Inhibit INBAND loopback in receive direction	—	—
INHLPBK-INBAND-TX (VTG301)	NSA	NR	Inhibit INBAND loopback in transmit direction	—	—
INHPMREPT	NSA	NR	All scheduled PM reports inhibited	—	—
LOF (VTG301)	SA	NR	Loss-of-frame – RCV	SF	30
LOF (VTG301)	SA	NR	Loss-of-frame – TRMT	—	30
LOS	SA	MJ	Loss-of-signal – RCV	SF	30
LOS (VTG301)	SA	MJ	Loss-of-signal – TRMT	—	30
MTCE	NSA	MN	Removed from service for maintenance	ABN (NEP)	53
RAI (VTG301)	SA	NR	Remote alarm indication – RCV	—	30
RAI (VTG301)	SA	NR	Remote alarm indication – TRMT	—	30
T-BPV (VTG101/102)	NSA	NA	Threshold violation for bipolar errors* – NE RCV	—	—
T-CSSP (VTG301)	NSA	NA	Threshold violation for controlled slips* – FE RCV	—	—
T-CSSP (VTG301)	NSA	NA	Threshold violation for controlled slips* – FE TRMT	—	—
T-CVL (VTG301)	NSA	NA	Threshold violation for bipolar/excessive zero errors* – NE RCV	—	—
T-CVP (VTG301)	NSA	NA	Threshold violation for DS1 path errors (CRC6 errors)* – FE RCV	—	—
T-CVP (VTG301)	NSA	NA	Threshold violation for DS1 path errors (CRC6 or framing errors)*– NE RCV	—	—
T-CVP (VTG301)	NSA	NA	Threshold violation for DS1 path errors (CRC6 errors)* – FE TRMT	—	—

Table X. Facility: External T1 (DS1) on DMI102/301 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
T-CVP (VTG301)	NSA	NA	Threshold violation for DS1 path errors (CRC6 or framing errors)* – NE TRMT	—	—
T-ESL (VTG301)	NSA	NA	Threshold violation for line errored seconds* – FE RCV	—	—
T-ESL	NSA	NA	Threshold violation for PM line errored seconds* – NE RCV	—	—
T-ESL (VTG301)	NSA	NA	Threshold violation for line errored seconds* – FE TRMT	—	—
T-ESP (VTG301)	NSA	NA	Threshold violation for path errored seconds* – FE RCV	—	—
T-ESP (VTG301)	NSA	NA	Threshold violation for path errored seconds* – NE RCV	—	—
T-ESP (VTG301)	NSA	NA	Threshold violation for path errored seconds* – FE TRMT	—	—
T-ESP (VTG301)	NSA	NA	Threshold violation for path errored seconds* – NE TRMT	—	—
T-SASP (VTG301)	NSA	NA	Threshold violation for AIS seconds* – NE RCV	—	—
T-SASP (VTG301)	NSA	NA	Threshold violation for AIS seconds*– NE TRMT	—	—
T-SEFS (VTG301)	NSA	NA	Threshold violation for severed errored framing seconds* – FE RCV	—	—
T-SEFS (VTG301)	NSA	NA	Threshold violation for severed errored framing seconds* – FE TRMT	—	—
T-SESL	NSA	NA	Threshold violation for PM line severely errored seconds* – NE RCV	—	—
T-SESP (VTG301)	NSA	NA	Threshold violation for path severely errored seconds* – NE RCV	—	—
T-SESP (VTG301)	NSA	NA	Threshold violation for path severely errored seconds* – FE RCV	—	—
T-SESP (VTG301)	NSA	NA	Threshold violation for path severely errored seconds* – NE TRMT	—	—
T-SESP (VTG301)	NSA	NA	Threshold violation for path severely errored seconds* – FE TRMT	—	—

Table X. Facility: External T1 (DS1) on DMI102/301 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
T-UASP (VTG301)	NSA	NA	Threshold violation for path unavailable seconds* – NE RCV	—	—
T-UASP (VTG301)	NSA	NA	Threshold violation for path unavailable seconds* – FE RCV	—	—
T-UASP (VTG301)	NSA	NA	Threshold violation for path unavailable seconds* – NE TRMT	—	—
T-UASP (VTG301)	NSA	NA	Threshold violation for path unavailable seconds* – FE TRMT	—	—
ACTLPBK	—	Event/ Condition	Loopback is active	—	—
AINS	—	Event/ Condition	Automatic In-Service state	—	—
IS-AUTO	—	Event	Automatic OOS-MA to IS	—	—
TSA-n where: n = MONE, MONF, SPLTA, SPLTB, SPLTE, SPLTF, LOOPE, or LOOPF	—	Condition	Test session is active	—	—
TSN-n where: n = 1..999	—	Condition	Test session number *n* is active	—	—
CONNTESTACT (VTG301)	—	Condition	Test pattern (Idle or QRSS) is connected		
QRSS (VTG301)	—	Condition	Quasi-random pattern detected on receive facility		

* *Either 15-minute or 1-day Threshold Crossing Alert (TCA).*

Table Y. Facility: Embedded T1 (DS1) on LIF601

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AIS	SA	NR	Alarm indication signal detected – RCV	SF	30
DS2OOF	SA	MJ	DS2 source out-of-frame	—	30
DS2RAI	SA	NR	DS2 source remote alarm indication	—	30
INHLPBK-DS2	NSA	NR	Inhibit DS2 loopback	—	—
INHLPBK-ESFLINE	NSA	NR	Inhibit ESFLINE loopback	—	—
INHLPBK-FEAC	NSA	NR	Inhibit FEAC loopback	—	—
INHPMREPT	NSA	NR	Inhibit PM report	—	—
LOF	SA	NR	Loss-of-frame	SF	30
MTCE	NSA	MN	Removed from service for maintenance	ABN (NEP)	53
RAI	SA	NR	Remote Alarm indication – RCV	—	30
T-CSSP	NSA	NA	Threshold violation for controlled slips – FE RCV*	—	—
T-CVP	NSA	NA	Threshold violation for Coding violation Path – NE RCV*	—	—
T-CVP	NSA	NA	Threshold violation forCoding violation Path – FE RCV*	—	—
T-ESL	NSA	NA	Threshold violation for line errored seconds – FE RCV*	—	—
T-ESP	NSA	NA	Threshold violation for path errored seconds – NE RCV*	—	—
T-ESP	NSA	NA	Threshold violation for path errored seconds – FE RCV*	—	—
T-SASP	NSA	NA	Threshold violation for AIS seconds – NE RCV*	—	—
T-SEFS	NSA	NA	Threshold violation for severed errored framing seconds – FE RCV*	—	—
T-SESP	NSA	NA	Threshold violation for path severely errored seconds – NE RCV*	—	—
T-SESP	NSA	NA	Threshold violation for path severely errored seconds – FE RCV*	—	—
T-UASP	NSA	NA	Threshold violation for path unavailable seconds – NE RCV*	—	—

Table Y. Facility: Embedded T1 (DS1) on LIF601

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
T-UASP	NSA	NA	Threshold violation for path unavailable seconds – FE RCV*	—	—
ACTLPBK	—	Condition/ Event	Loopback is active	—	—
AINS	—	Condition/ Event	Automatic In-Service state	—	—
IS-AUTO	—	Event	Automatic OOS-MA to IS	—	—
* *Either 15-minutes or 1-day Threshold Crossing Alert (TCA).*					

Table Z. Facility: T3 (DS3) on LIF301

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
BERL-HT	SA	CR	Signal failure bit error rate threshold crossed	SF	30
INHPMREPT	NSA	NR	All scheduled PM reports inhibited	—	—
LOS	SA	CR	Loss-of-signal	SF	30
MTCE	NSA	MN	Removed from service for maintenance	ABN (NEP)	53
T-BPV	NSA	NA	Threshold violation for bipolar errors* – RCV NE	—	—
T-ESL	NSA	NA	Threshold violation for PM line errored seconds* – RCV NE	—	—
T-SESL	NSA	NA	Threshold violation for PM line severely errored seconds* – RCV NE	—	—
ACTLPBK	—	Condition/ Event	Loopback is active	—	—
AINS	—	Condition/ Event	Automatic In-Service state	—	—
IS-AUTO	—	Event	Automatic OOS-MA to IS	—	—
CONNTESTACT	—	Condition	Test active (IDLE or quasi-random data)		
* *Either 15-minute or 1-day Threshold Crossing Alert (TCA).*					

Table AA. Facility: T3 (DS3) on LIF501/701/D01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AIS	SA	NR	Alarm indication signal – RCV NE	SF	30
AIS	SA	NR	Alarm indication signal – TRMT NE	—	30
BERL-HT	SA	CR	Signal failure bit error rate threshold crossed	SF	30
INHPMREPT	NSA	NR	All scheduled PM reports inhibited	—	—
LOF	SA	NA	Loss-of-frame – RCV NE	SF	30
LOF	SA	NA	Loss-of-frame – TRMT NE	—	30
LOS	SA	CR	Loss-of-signal	SF	30
MTCE	NSA	MN	Removed from service for maintenance	ABN (NEP)	53
T-CVL	NSA	NA	Coding violation Line TCA [1] – RCV NE	—	—
T-CVCPP	NSA	NA	Threshold violation for CP-bit errors [1] – RCV NE	—	—
T-CVCPP	NSA	NA	Threshold violation for CP-bit path errors [1] – TRMT NE	—	—
T-CVPP	NSA	NA	Threshold violation for P-bit path errors [1] – RCV NE	—	—
T-CVPP	NSA	NA	Threshold violation for P-bit path errors [1] – TRMT NE	—	—
T-ESCPP	NSA	NA	Threshold violation for CP-bit path errored seconds [1] – RCV NE	—	—
T-ESCPP	NSA	NA	Threshold violation for CP-bit path errored seconds [1] – TRMT NE	—	—
T-ESL	NSA	NA	Threshold violation for PM line errored seconds [1] – RCV NE	—	—
T-ESPP	NSA	NA	Threshold violation for P-bit path errored seconds [1] – RCV NE	—	—
T-ESPP	NSA	NA	Threshold violation for P-bit path errored seconds [1] – TRMT NE	—	—
T-SASP	NSA	NA	Threshold violation for SEF/AIS seconds [1] – RCV NE	—	—
T-SASP	NSA	NA	Threshold violation for SEF/AIS seconds [1] – TRMT NE	—	—
T-SESCPP	NSA	NA	Threshold violation for CP-bit path severely errored seconds [1] – RCV NE	—	—

Table AA. Facility: T3 (DS3) on LIF501/701/D01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
T-SESCPP	NSA	NA	Threshold violation for CP-bit path severely errored seconds [1] – TRMT NE	—	—
T-SESL	NSA	NA	Threshold violation for PM line severely errored seconds [1] – RCV NE	—	—
T-SESPP	NSA	NA	Threshold violation for P-bit severely errored seconds [1] – RCV NE	—	—
T-SESPP	NSA	NA	Threshold violation for P-bit path severely errored seconds [1] – TRMT NE	—	—
T-UASCPP	NSA	NA	Threshold violation for CP-bit path unavailable seconds [1] – RCV NE	—	—
T-UASCPP	NSA	NA	Threshold violation for CP-bit path unavailable seconds [1] – TRMT NE	—	—
T-UASPP	NSA	NA	Threshold violation for P-bit path unavailable seconds [1] – RCV NE	—	—
T-UASPP	NSA	NA	Threshold violation for P-bit path unavailable seconds [1] – TRMT NE	—	—
ACTLPBK	—	Condition/ Event	Loopback is active	—	—
AINS	—	Condition/ Event	Automatic In-Service state	—	—
IS-AUTO	—	Event	Automatic OOS-MA to IS	—	—
CONNTESTACT	—	Condition	Test active (IDLE or quasi-random data)		
DS3AIS [2]	—	Condition	DS3 AIS type detected		

[1] *Either 15-minute or 1-day Threshold Crossing Alert (TCA).*

[2] *DS3 AIS type is displayed as comment:*
1010 with stuck stuffing (NAS)
1010 without stuck stuffing (BLUE)

Table AB. Facility: T3 (DS3) on LIF601

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AIS	SA	NR	Alarm indication signal – RCV	SF	30
BERL-HT	SA	CR	Signal failure bit error rate threshold crossed	SF	30
FRMMF	SA	MN	Frame format mismatch	—	30
ISD	SA	NR	Idle pattern detected – RCV NE	—	30
INHPMREPT	NSA	NR	All scheduled PM reports inhibited	—	—
INHLPBK	NSA	NR	Inhibit Loopback	—	—
LOF	SA	CR	Loss-of-frame – RCV	SF	30
LOS	SA	CR	Loss-of-signal	SF	30
MTCE	NSA	MN	Removed from service for maintenance	ABN (NEP)	53
RAI	SA	NR	Remote alarm indication	—	30
RAIXBIT	SA	NR	Remote alarm indication – based on X-bits	—	30
T-CVCPP	NSA	NA	Threshold violation for CP-bit path errors [1] – RCV NE	—	—
T-CVCPP	NSA	NA	Threshold violation for CP-bit path errors [1] – RCV FE	—	—
T-CVL	NSA	NA	Threshold violation for line coding errors [1] – RCV NE	—	—
T-CVPP	NSA	NA	Threshold violation for P-bit path errors [1] – RCV NE	—	—
T-ESCPP	NSA	NA	Threshold violation for CP-bit path errored seconds [1] – RCV NE	—	—
T-ESCPP	NSA	NA	Threshold violation for CP-bit path errored seconds [1] – RCV FE	—	—
T-ESL	NSA	NA	Threshold violation for PM line errored seconds [1] – RCV NE	—	—
T-ESPP	NSA	NA	Threshold violation for P-bit path errored seconds [1] – RCV NE	—	—
T-SASCP	NSA	NA	Threshold violation for SEF/AIS seconds based on X-bits [1] – RCV FE	—	—
T-SASP	NSA	NA	Threshold violation for SEF/AIS seconds [1] – RCV NE	—	—
T-SESCPP	NSA	NA	Threshold violation for CP-bit path severely errored seconds [1] – RCV NE	—	—

Table AB. Facility: T3 (DS3) on LIF601 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
T-SESCPP	NSA	NA	Threshold violation for CP-bit path severely errored seconds [1] –RCV FE	—	—
T-SESL	NSA	NA	Threshold violation for PM line severely errored seconds [1] – RCV NE	—	—
T-SESPP	NSA	NA	Threshold violation for P-bit path severely errored seconds [1] – RCV NE	—	—
T-UASCPP	NSA	NA	Threshold violation for CP-bit path unavailable seconds [1] – RCV NE	—	—
T-UASCPP	NSA	NA	Threshold violation for CP-bit path unavailable seconds [1] – RCV FE	—	—
T-UASPP	NSA	NA	Threshold violation for P-bit path unavailable seconds [1] – RCV NE	—	—
ACTLPBK	—	Condition/ Event	Loopback is active	—	—
AINS	—	Condition/ Event	Automatic-In-Service state	—	—
IS-AUTO	—	Event	Automatic OOS-MA to IS	—	—
CONNTESTACT	—	Condition	Test active (IDLE or quasi-random data)	—	—
DS3AIS [2]	—	Condition	DS3 AIS type detected	—	—
FEAC-( ) [3] where ( ) = 6 character string representing FEAC binary code	—	Condition	Far-end alarm and control received	—	—
QRSS	—	Condition	Quasi-random pattern detected on receive facility	—	—

[1] *Either 15-minute or 1-day Threshold Crossing Alert (TCA).*

[2] *DS3 AIS type is displayed as comment:*
0101 with stuck stuffing
0101 without stuck stuffing
1010 with stuck stuffing (NAS)
1010 without stuck stuffing (BLUE)

[3] *The translation of FEAC binary code is displayed as comment: DS3EQPT-SA, DS3LOS, DS3OOF, DS3AIS, DS3IDLE, DS3EQPT-NSA, COMMEQPT-NSA, MDS1LOS, DS1EQPT-SA, DS1LOS, DS1EQPT-NSA, or UNDEFINED.*

Table AC. Facility: SMI (BITS)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AIS	NSA	NR	Alarm indication signal detected	—	—
AISYEL	NSA	NR	AIS yellow detected	—	—
BER-HT	NSA	MN	Bit error ratio – high threshold crossed	—	—
LOF	NSA	MN	Loss-of-frame	—	—
LOS	NSA	MN	Loss-of-signal	—	—
MTCE	NSA	MN	Removed from service for maintenance	ABN (NEP)	53
SYNCLEVINFAIL	NSA	MN	Synchronization message failure	—	—
YEL	NSA	NR	Yellow (facility) detected	—	—
SYNCLEVINCHG	—	NA*	Synchronization level input change	—	—
SYNCLEVIN-n where: n = 0...47	—	Condition	Value of synchronization input level	—	—
SYNCLEVOUT-n where: n = 0...47	—	Condition	Value of synchronization input level	—	—
* *The SYNCLEVINCHG event can only be provisioned as NA or NR.*					

Table AD. Line Group: STS Path on HIFB01/60x/F01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AISP	SA	NR/NR	Path alarm indication signal detected	—	—
BERP-HT	NSA	NA/NA	Bit error ratio high threshold	—	—
BERP-LT	NSA	NA/NA	Bit error ratio low threshold	—	—
BLSRPATHNA [1]	SA	MJ/MN	BLSR path not available	—	—
BRIDGE [1]	NSA	MN/MN	Working or protection is bridged	—	—
CONCAT	SA	MJ/MN	Concatenation mismatch	—	—
FRCD [2]	NSA	MN/MN	Ring forced switch request	ABN (NEP)	42 & 53
FRCDWKSWBK [2]	NSA	NR/NR	Protected path forced switch back	—	—

Table AD. Line Group: STS Path on HIFB01/60x/F01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
FRCDWKSWPR [2]	NSA	NR/NR	Protected path forced switch to protecting path	—	—
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
LOCKOUT [2]	NSA	MN/MN	Lockout of protection/working switch request	ABN (NEP)	42 & 53
LOMF [3]	SA	MJ/MN	Loss-of-multiframe	—	—
LOP	SA	MJ/MN	Loss-of-pointer	—	—
MAN [2]	NSA	MN/MN	Ring manual switch request	ABN (NEP)	42 & 53
MANWKSBK [2]	NSA	NR/NR	Manual switch back to protected	—	—
MANWKSPR [2]	NSA	NR/NR	Manual switch of protected path to protecting path	—	—
PATHSEL [2]	SA	CR/CR	Both paths failed, did not switch	—	43
PDI	SA	NR/NR	Payload defect indication	—	—
PLM	SA	MN/MN	Payload label mismatch	—	—
PROTNA [2]	NSA	MN/MN	Protection not available	—	—
RFI [4]	SA	NR/NR	Path yellow	—	—
RFIMM [4]	SA	MN/MN	Remote failure indicator mismatch	—	—
SQUELCH (RCV) [1]	SA	CR/MN	Squelch RCV traffic	—	—
SQUELCH (TRMT) [1]	SA	CR/MN	Squelch TRMT traffic	—	—
TIM [3]	NSA	MN/MN	Trace identifier message failure	—	—
T-CVP [4]	NSA	NA/NA	Threshold violation for PM STS path BIP errors [6] – NE	—	—
T-CVP [4]	NSA	NA/NA	Threshold violation for PM STS path BIP errors [6] – FE	—	—
T-ESP [4]	NSA	NA/NA	Threshold violation for PM STS path error seconds [6] – NE	—	—
T-ESP [4]	NSA	NA/NA	Threshold violation for PM STS path error seconds [6] – FE	—	—
T-NPJCDET	NSA	NA/NA	Threshold violation for PM STS negative pointer justification count detected[6] – NE	—	—
T-NPJCGEN	NSA	NA/NA	Threshold violation for PM STS negative pointer justification count generated [6] – NE	—	—

Table AD. Line Group: STS Path on HIFB01/60x/F01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
T-PPJCDET	NSA	NA/NA	Threshold violation for PM STS positive pointer justification count detected [6] – NE	—	—
T-PPJCGEN	NSA	NA/NA	Threshold violation for PM STS positive pointer justification count generated [6] – NE	—	—
T-PJCSDET	NSA	NA/NA	Threshold violation for PM STS pointer justification count seconds detected [6] – NE	—	—
T-PJCSGEN	NSA	NA/NA	Threshold violation for PM STS pointer justification count generated [6] – NE	—	—
T-PJCDIFF	NSA	NA/NA	Threshold violation for PM STS pointer justification count difference [6] – NE	—	—
T-SESP [4]	NSA	NA/NA	Threshold violation for PM STS path severely errored seconds [6] – NE	—	—
T-SESP [4]	NSA	NA/NA	Threshold violation for PM STS path severely errored seconds [6] – FE	—	—
T-UASP [4]	NSA	NA/NA	Threshold violation for PM STS path unavailable seconds [6] – NE	—	—
T-UASP [4]	NSA	NA/NA	Threshold violation for PM STS path unavailable seconds [6] – FE	—	—
UNEQ	SA	MN/MN	STS path unequipped	—	—
WKSWBK [2]	NSA	NR/NR	Protected path switch back		
WKSWPR [2]	NSA	NR/NR	Switch of protected path to protecting path	—	—
BLSR [1]	—	Event	BLSR switch reason	—	—
BUERR	—	Event	Switch reason: star fail	—	—
TIMCHG [3]	—	Event	Trace identifier message changed	—	—
WTRREVERT [2]	—	Event	Switch reason: Wait to restore timeout (revert)	—	—
ERDI-xxx [5] where xxx =3 bit RDI	—	Condition	Enhanced remote defect indicator	—	—
PROTECTED-ACT [2]	—	Condition	Protected path is active	—	—

Table AD. Line Group: STS Path on HIFB01/60x/F01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTING-ACT [2]	—	Condition	Protecting path is active	—	—
PROTECTED-ALL [2]	—	Condition	Protected path conditions (TL1 input only)	—	—
PROTECTING-ALL [2]	—	Condition	Protecting path conditions (TL1 input only)	—	—
PROTECTED-BLSRFAIL [2]	—	Condition	Protected path fails due to BLSR	—	—
PROTECTING-BLSRFAIL [2]	—	Condition	Protecting path fails due to BLSR	—	—
PROTECTED-DG1 [2]	—	Condition	Protected path is Drop Group 1	—	—
PROTECTING-DG1 [2]	—	Condition	Protecting path is Drop Group 1	—	—
PROTECTED-DG2 [2]	—	Condition	Protected path is Drop Group 2	—	—
PROTECTING-DG2 [2]	—	Condition	Protecting path is Drop Group 2	—	—
PROTECTED-DG3 [2]	—	Condition	Protected path is Drop Group 3	—	—
PROTECTING-DG3 [2]	—	Condition	Protecting path is Drop Group 3	—	—
PROTECTED-DG4 [2]	—	Condition	Protected path is Drop Group 4	—	—
PROTECTING-DG4 [2]	—	Condition	Protecting path is Drop Group 4	—	—
PROTECTED-DG1A [2]	—	Condition	Protected path is Drop Group 1A	—	—
PROTECTING-DG1A [2]	—	Condition	Protecting path is Drop Group 1A	—	—
PROTECTED-DG2A [2]	—	Condition	Protected path is Drop Group 2A	—	—
PROTECTING-DG2A [2]	—	Condition	Protecting path is Drop Group 2A	—	—
PROTECTED-DG3A [2]	—	Condition	Protected path is Drop Group 3A	—	—
PROTECTING-DG3A [2]	—	Condition	Protecting path is Drop Group 3A	—	—
PROTECTED-DG4A [2]	—	Condition	Protected path is Drop Group 4A	—	—
PROTECTING-DG4A [2]	—	Condition	Protecting path is Drop Group 4A	—	—
PROTECTED-DG1B [2]	—	Condition	Protected path is Drop Group 1B	—	—
PROTECTING-DG1B [2]	—	Condition	Protecting path is Drop Group 1B	—	—

Table AD. Line Group: STS Path on HIFB01/60x/F01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTED-DG2B [2]	—	Condition	Protected path is Drop Group 2B	—	—
PROTECTING-DG2 [2]	—	Condition	Protecting path is Drop Group 2B	—	—
PROTECTED-DG3B [2]	—	Condition	Protected path is Drop Group 3B	—	—
PROTECTING-DG3B [2]	—	Condition	Protecting path is Drop Group 3B	—	—
PROTECTED-DG4B [2]	—	Condition	Protected path is Drop Group 4B	—	—
PROTECTING-DG4B [2]	—	Condition	Protecting path is Drop Group 4B	—	—
PROTECTED-FAIL [2]	—	Condition	Protected path failed	—	—
PROTECTING-FAIL [2]	—	Condition	Protecting path failed	—	—
PROTECTED-FRCD [2]	—	Condition	Protected path has forced switch	—	—
PROTECTING-FRCD [2]	—	Condition	Protecting path has forced switch	—	—
PROTECTED-LG1 [2]	—	Condition	Protected path is Line Group 1	—	—
PROTECTING-LG1 [2]	—	Condition	Protecting path is Line Group 1	—	—
PROTECTED-LG2 [2]	—	Condition	Protected path is Line Group 2	—	—
PROTECTING-LG2 [2]	—	Condition	Protecting path is Line Group 2	—	—
PROTECTED-LOCKOUT [2]	—	Condition	Lockout switch required on protected path	—	—
PROTECTING-LOCKOUT [2]	—	Condition	Lockout switch required on protecting path	—	—
PROTECTED-MAN [2]	—	Condition	Protected path has manual switch	—	—
PROTECTING-MAN[2]	—	Condition	Protecting path has manual switch	—	—
PROTECTED-RFI [2]	—	Condition	Protected path has RFIP	—	—
PROTECTING-RFI [2]	—	Condition	Protecting path has RFIP	—	—
PROTECTED-STBY [2]	—	Condition	Protected path is standby	—	—
PROTECTING-STBY [2]	—	Condition	Protecting path is standby	—	—
PROTECTED-UNEQ [2]	—	Condition	Protected path is UNEQ (signal label)	—	—
PROTECTING-UNEQ [2]	—	Condition	Protecting path is unequipped (signal label)	—	—

Table AD. Line Group: STS Path on HIFB01/60x/F01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
SIGLBL-xxx (RCV) where xxx =0...255	—	Condition	Received path signal label	—	—
SIGLBL-xxx (TRMT) [7] where xxx =0...255	—	Condition	Transmit PDI	—	—
Protected−PD1 [2]	—	Condition	Protected path has PD1	—	—
Protecting−PD1 [2]	—	Condition	Protecting path has PD1	—	—

[1] *BLSR only.*

[2] *UPSR ring only.*

[3] *Applicable only to STS terminated path that is provisioned for VT payload.*

[4] *Applicable only when intermediate STS path enabled or STS path terminated.*

[5] *Applicable only when 3 bit RDI is enabled and when intermediate STS path enabled or STS path terminated.*

[6] *Either 15-minutes or 1-day Threshold Crossing Alert (TCA).*

[7] *Applicable only when PDI generation is enabled.*

Table AE. Line Group: VT Path on HIFB01/60x/F01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AISP	SA	NR/NR	Alarm indication signal detected	—	—
BERP-HT	NSA	NA/NA	Path failure − Bit error rate threshold crossed	—	—
BERP-LT	NSA	NA/NA	Path degraded − Bit error ratio threshold crossed	—	—
FRCD [1]	NSA	MN/MN	Ring forced switch request	ABN (NEP)	42 & 53
FRCDWKSWBK [1]	NSA	NR/NR	Protected path forced switch back	—	—
FRCDWKSWPR [1]	NSA	NR/NR	Protected path forced switch to protecting path	—	—
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
LOCKOUT [1]	NSA	MN/MN	Lock out of protection/working switch request	ABN (NEP)	42 & 53
LOP	SA	MJ/MN	VT loss-of-pointer	—	—

Table AE. Line Group: VT Path on HIFB01/60x/F01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
MAN [1]	NSA	MN/MN	Ring manual switch request	ABN (NEP)	42 & 53
MANWKSBK [1]	NSA	NR/NR	Manual switch back to protected	—	—
MANWKSPR [1]	NSA	NR/NR	Manual switch of protected path to protecting path	—	—
PATHSEL [1]	SA	MJ/MJ	Both paths failed, did not switch	—	43
PLM	NSA	MN/MN	Payload label mismatch	—	—
PROTNA [1]	NSA	MN/NN	Protection not available	—	—
T-NPJCDET [2]	NSA	NA/NA	Threshold violation for PM VT negative pointer justification count detected [3] – NE	—	—
T-NPJCGEN [2]	NSA	NA/NA	Threshold violation for PM VT negative pointer justification count generated [3] – NE	—	—
T-PPJCDET [2]	NSA	NA/NA	Threshold violation for PM VT positive pointer justification count detected [3] – NE	—	—
T-PPJCGEN [2]	NSA	NA/NA	Threshold violation for PM VT positive pointer justification count generated [3] – NE	—	—
T-PJCSDET [2]	NSA	NA/NA	Threshold violation for PM VT pointer justification count seconds detected [3] – NE	—	—
T-PJCSGEN [2]	NSA	NA/NA	Threshold violation for PM VT pointer justification count seconds generated [3] – NE	—	—
T-PJCDIFF [2]	NSA	NA/NA	Threshold violation for PM VT pointer justification count difference [3] – NE	—	—
UNEQ	NSA	MN/MN	Path unequipped	—	—
VTSIZE	SA	MJ/MN	VT size mismatch	—	—
WKSWBK [1]	NSA	NR/NR	Protected path switch back		
WKSWPR [1]	NSA	NR/NR	Switch of protected path to protecting path	—	—
WTRREVERT [1]	—	Event	Switch Reason: Wait to restore timeout (in revertive mode)	—	—
PROTECTED-ACT [1]	—	Condition	Protected path is active	—	—
PROTECTING-ACT [1]	—	Condition	Protecting path is active	—	—

Table AE. Line Group: VT Path on HIFB01/60x/F01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTED-ALL [1]	—	Condition	Protected path conditions (TL1 input only)	—	—
PROTECTING-ALL [1]	—	Condition	Protecting path conditions (TL1 input only)	—	—
PROTECTED-DG1 [1]	—	Condition	Protected path is Drop Group 1	—	—
PROTECTING-DG1 [1]	—	Condition	Protecting path is Drop Group 1	—	—
PROTECTED-DG2 [1]	—	Condition	Protected path is Drop Group 2	—	—
PROTECTING-DG2 [1]	—	Condition	Protecting path is Drop Group 2	—	—
PROTECTED-DG3 [1]	—	Condition	Protected path is Drop Group 3	—	—
PROTECTING-DG3 [1]	—	Condition	Protecting path is Drop Group 3	—	—
PROTECTED-DG4 [1]	—	Condition	Protected path is Drop Group 4	—	—
PROTECTING-DG4 [1]	—	Condition	Protecting path is Drop Group 4	—	—
PROTECTED-DG1A [1]	—	Condition	Protected path is Drop Group 1A	—	—
PROTECTING-DG1A [1]	—	Condition	Protecting path is Drop Group 1A	—	—
PROTECTED-DG2A [1]	—	Condition	Protected path is Drop Group 2A	—	—
PROTECTING-DG2A [1]	—	Condition	Protecting path is Drop Group 2A	—	—
PROTECTED-DG3A [1]	—	Condition	Protected path is Drop Group 3A	—	—
PROTECTING-DG3A [1]	—	Condition	Protecting path is Drop Group 3A	—	—
PROTECTED-DG4A [1]	—	Condition	Protected path is Drop Group 4A	—	—
PROTECTING-DG4A [1]	—	Condition	Protecting path is Drop Group 4A	—	—
PROTECTED-DG1B [1]	—	Condition	Protected path is Drop Group 1B	—	—
PROTECTING-DG1B [1]	—	Condition	Protecting path is Drop Group 1B	—	—
PROTECTED-DG2B [1]	—	Condition	Protected path is Drop Group 2B	—	—
PROTECTING-DG2B [1]	—	Condition	Protecting path is Drop Group 2B	—	—
PROTECTED-DG3B [1]	—	Condition	Protected path is Drop Group 3B	—	—

Table AE. Line Group: VT Path on HIFB01/60x/F01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTING-DG3B [1]	—	Condition	Protecting path is Drop Group 3B	—	—
PROTECTED-DG4B [1]	—	Condition	Protected path is Drop Group 4B	—	—
PROTECTING-DG4B [1]	—	Condition	Protecting path is Drop Group 4B	—	—
PROTECTED-FAIL [1]	—	Condition	Protected path is failed	—	—
PROTECTING-FAIL [1]	—	Condition	Protecting path is failed	—	—
PROTECTED-FRCD [1]	—	Condition	Protected path has forced switch	—	—
PROTECTING-FRCD [1]	—	Condition	Protecting path has forced switch	—	—
PROTECTED-LG1 [1]	—	Condition	Protected path is Line Group 1	—	—
PROTECTING-LG1 [1]	—	Condition	Protecting path is Line Group 1	—	—
PROTECTED-LG2 [1]	—	Condition	Protected path is Line Group 2	—	—
PROTECTING-LG2 [1]	—	Condition	Protecting path is Line Group 2	—	—
PROTECTED-LOCKOUT [1]	—	Condition	Lockout switch required on protected path	—	—
PROTECTING-LOCKOUT [1]	—	Condition	Lockout switch required on protecting path	—	—
PROTECTED-MAN [1]	—	Condition	Protected path has manual switch	—	—
PROTECTING-MAN [1]	—	Condition	Protecting path has manual switch	—	—
PROTECTED-RFI [1]	—	Condition	Protected path has RFIP	—	—
PROTECTING-RFI [1]	—	Condition	Protecting path has RFIP	—	—
PROTECTED-STBY [1]	—	Condition	Protected path is standby	—	—
PROTECTING-STBY [1]	—	Condition	Protecting path is standby	—	—
PROTECTED-UNEQ [1]	—	Condition	Protected path is UNEQ (signal label)	—	—
PROTECTING-UNEQ [1]	—	Condition	Protecting path is unequipped (signal label)	—	—
SIGLBL-x where x = VT signal label code	—	Condition	VT path signal label code	—	—

[1] *UPSR ring only.*

[2] *Alarm reported only against selected VT.*

[3] *Either 15-minutes or 1-day Threshold Crossing Alert (TCA).*

Table AF. Drop Group: STS Path on LIF201/301/501/701/D01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AISP (RCV & TRMT)	SA	NR	Path alarm indication signal detected	—	—
BERP-HT	NSA	NA	Bit error ratio high threshold	—	—
BERP-LT	NSA	NA	Bit error ratio low threshold	—	—
ETFAIL	SA	MJ	Extra traffic failed on BLSR ring	—	—
FRCD [1]	NSA	MN	Forced switch requested on UPSR ring	ABN	42 & 53
FRCDWKSWBK [1]	NSA	NR	Protected path forced switch back	—	—
FRCDWKSWPR [1]	NSA	NR	Protected path forced switch to protecting	—	—
INHPMREPT	NSA	NR	All scheduled PM reports inhibited	—	—
LOCKOUT [1]	NSA	MN	Lockout requested on UPSR ring	ABN	42 & 53
LOMF [2] [7]	SA	MJ	STS loss-of-multiframe	—	—
LOP (RCV & TRMT)	SA	MJ	STS loss-of-pointer	—	—
MAN [1]	NSA	MN	Manual switch requested on UPSR ring	ABN	42 & 53
MANWKSWBK [1]	NSA	NR	Manual switch back to protected	—	—
MANWKSWPR [1]	NSA	NR	Manual switch of protected to protecting	—	—
PATHSEL [1]	SA	CR	Both paths failed, did not switch	—	43
PDI (RCV & TRMT) [2] [6]	SA	NR	Payload defect indication	—	—
PLM (RCV & TRMT) [2]	SA	MN	Payload label mismatch	—	—
PROTNA [1]	NSA	MN	Protection not available	—	—
RFI (RCV & TRMT) [2]	SA	NR	STS path yellow	—	—
TIM [2]	NSA	MN	Trace identifier message failure	—	—
T-CVP [3]	NSA	NA	Threshold violation for PM STS path BIP errors [4] – NE	—	—
T-CVP [3]	NSA	NA	Threshold violation for PM STS path BIP errors [4] – FE	—	—
T-ESP [3]	NSA	NA	Threshold violation for PM STS path error seconds [4] – NE	—	—
T-ESP [3]	NSA	NA	Threshold violation for PM STS path error seconds [4] – FE	—	—
T-NPJCDET [7]	NSA	NA	Threshold violation for PM STS negative pointer justification count detected [4] – NE	—	—

Table AF. Drop Group: STS Path on LIF201/301/501/701/D01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
T-NPJCGEN [6]	NSA	NA	Threshold violation for PM STS negative pointer justification count generated [4] – NE	—	—
T-PPJCDET [7]	NSA	NA	Threshold violation for PM STS positive pointer justification count detected [4] – NE	—	—
T-PPJCGEN [6]	NSA	NA	Threshold violation for PM STS positive pointer justification count generated [4] – NE	—	—
T-PJCSDET [6] [7]	NSA	NA	Threshold violation for PM STS pointer justification count seconds detected [4] – NE	—	—
T-PJCSGEN [6] [7]	NSA	NA	Threshold violation for PM STS pointer justification count generated [4] – NE	—	—
T-PJCDIFF [6] [7]	NSA	NA	Threshold violation for PM STS pointer justification count difference [4] – NE	—	—
T-SESP [3]	NSA	NA	Threshold violation for PM STS path severely errored seconds [4] – NE	—	—
T-SESP [3]	NSA	NA	Threshold violation for PM STS path severely errored seconds [4] – FE	—	—
T-UASP [3]	NSA	NA	Threshold violation for PM STS path unavailable seconds [4] – NE	—	—
T-UASP [3]	NSA	NA	Threshold violation for PM STS path unavailable seconds [4] – FE	—	—
UNEQ (RCV) [2]	SA	MN	STS path unequipped	—	—
UNEQ (TRMT) [2]	SA	MN	STS path unequipped	—	—
WKSWBK [1]	NSA	NR /NA	Protected path switch back	—	—
WKSWPR [1]	NSA	NR /NA	Protected path switch to protection	—	—
BLSR	—	Event	BLSR ring switch reason	—	—
TIMCHG [2]	—	Event	Trace message identification change	—	—
WTRREVERT [1]	—	Event	Wait to revert time out on UPSR ring (switch reason)	—	—
PROTECTED-ACT [1]	—	Condition	Protected path is active	—	—

Table AF. Drop Group: STS Path on LIF201/301/501/701/D01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTING-ACT [1]	—	Condition	Protecting path is active	—	—
PROTECTED-ALL [1]	—	Condition	Protected path conditions (TL1 input only)	—	—
PROTECTING-ALL [1]	—	Condition	Protecting path conditions (TL1 input only)	—	—
PROTECTED-BLSRFAIL [1]	—	Condition	Protected path fails due to BLSR	—	—
PROTECTING-BLSRFAIL [1]	—	Condition	Protecting path fails due to BLSR	—	—
PROTECTED-DG1 [1]	—	Condition	Protected path is Drop Group 1	—	—
PROTECTING-DG1 [1]	—	Condition	Protecting path is Drop Group 1	—	—
PROTECTED-DG2 [1]	—	Condition	Protected path is DropjGroup 2	—	—
PROTECTING-DG2 [1]	—	Condition	Protecting path is Drop Group 2	—	—
PROTECTED-DG3 [1]	—	Condition	Protected path is Drop Group 3	—	—
PROTECTING-DG3 [1]	—	Condition	Protecting path is Drop Group 3	—	—
PROTECTED-DG4 [1]	—	Condition	Protected path is Drop Group 4	—	—
PROTECTING-DG4 [1]	—	Condition	Protecting path is Drop Group 4	—	—
PROTECTED-DG1A [1]	—	Condition	Protected path is Drop Group 1A	—	—
PROTECTING-DG1A [1]	—	Condition	Protecting path is Drop Group 1A	—	—
PROTECTED-DG2A [1]	—	Condition	Protected path is DropjGroupA 2A	—	—
PROTECTING-DG2A [1]A	—	Condition	Protecting path is Drop Group 2A	—	—
PROTECTED-DG3A [1]	—	Condition	Protected path is Drop Group 3A	—	—
PROTECTING-DG3A [1]	—	Condition	Protecting path is Drop Group 3A	—	—
PROTECTED-DG4A [1]	—	Condition	Protected path is Drop Group 4A	—	—
PROTECTING-DG4A [1]	—	Condition	Protecting path is Drop GroupA 4A	—	—
PROTECTED-DG1B [1]	—	Condition	Protected path is Drop Group 1B	—	—
PROTECTING-DG1B [1]	—	Condition	Protecting path is Drop Group 1B	—	—
PROTECTED-DG2B [1]	—	Condition	Protected path is DropjGroup 2B	—	—

Table AF. Drop Group: STS Path on LIF201/301/501/701/D01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTING-DG2B [1]	—	Condition	Protecting path is Drop Group 2B	—	—
PROTECTED-DG3B [1]	—	Condition	Protected path is Drop Group 3B	—	—
PROTECTING-DG3B [1]	—	Condition	Protecting path is Drop Group 3B	—	—
PROTECTED-DG4B [1]	—	Condition	Protected path is Drop Group 4B	—	—
PROTECTING-DG4B [1]	—	Condition	Protecting path is Drop Group 4B	—	—
PROTECTED-FAIL [1]	—	Condition	Protected path is failed	—	—
PROTECTING-FAIL [1]	—	Condition	Protecting path is failed	—	—
PROTECTED-FRCD [1]	—	Condition	Protected path has forced switch	—	—
PROTECTING-FRCD [1]	—	Condition	Protecting path has forced switch	—	—
PROTECTED-LG1 [1]	—	Condition	Protected path is Line Group 1	—	—
PROTECTING-LG1 [1]	—	Condition	Protecting path is Line Group 1	—	—
PROTECTED-LG2 [1]	—	Condition	Protected path is Line Group 2	—	—
PROTECTING-LG2 [1]	—	Condition	Protecting path is Line Group 2	—	—
PROTECTED-LOCKOUT [1]	—	Condition	Lockout switch request on protected path	—	—
PROTECTING-LOCKOUT [1]	—	Condition	Lockout switch request on protecting path	—	—
PROTECTED-MAN [1]	—	Condition	Protected path has manual switch	—	—
PROTECTING-MAN [1]	—	Condition	Protecting path has manual switch	—	—
PROTECTED-PDI [1]	—	Condition	PDI being received on protected path	—	—
PROTECTING-PDI [1]	—	Condition	PDI being received on protecting path	—	—
PROTECTED-RFI [1]	—	Condition	Protected path has RFIP	—	—
PROTECTING-RFI [1]	—	Condition	Protecting path has RFIP	—	—
PROTECTED-STBY [1]	—	Condition	Protected path is standby	—	—
PROTECTING-STBY [1]	—	Condition	Protecting path is standby	—	—
PROTECTED-UNEQ [1]	—	Condition	Protected path is UNEQ (signal label)	—	—
PROTECTING-UNEQ [1]	—	Condition	Protecting path is UNEQ (signal label)	—	—

Table AF. Drop Group: STS Path on LIF201/301/501/701/D01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
SIGLBL-xxx (RCV) where xxx = 0...255	—	Condition	Receive path signal label	—	—
SIGLBL-xxx (TRMT) where xxx = 0...255 [5]	—	Condition	Transmit PDI	—	—

[1] *UPSR ring only.*

[2] *This alarm only applies to an STS terminated path which carries a VT payload or DS3 payload.*

[3] *This alarm only applies to an intermediate STS path that is enabled or terminated (VT payload or DS3 payload).*

[4] *Either 15-minute or 1-day Threshold Crossing Alert (TCA).*

[5] *This condition only applies when PDI generation is enabled.*

[6] *Does not apply to LIF201*

[7] *Does not apply to LIF301*

Table AG. Drop Group: STS Path on LIF401/404/F01/A01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [8]	DESCRIPTION	LED	SERIAL E2A BIT
AISP	SA	NR/NR	STS path AIS (Alarm Indication Signal)	—	—
BERP-HT (TRMT)	NSA	NA/NA	Bit error ratio high threshold	—	—
BERP-LT (TRMT)	NSA	NA/NA	Bit error ratio low threshold	—	—
CONCAT	SA	MJ/MN	Concatenation mismatch	—	—
ETFAIL	SA	MJ/MN	Extra traffic failed on BLSR ring	—	—
FRCD [1]	NSA	MN/MN	Forced switch requested on UPSR ring	ABN	42 & 53
FRCDWKSWBK [1]	NSA	NR/NR	Protected path forced switch back	—	—
FRCDWKSWPR [1]	NSA	NR/NR	Protected path forced switch to protecting path	—	—
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
LOCKOUT [1]	NSA	MN/MN	Lockout requested on UPSR ring	ABN	42 & 53
LOMF [2]	SA	MJ/MN	STS loss-of-multiframe	—	—
LOP	SA	MJ/MN	STS loss-of-pointer	—	—

Table AG. Drop Group: STS Path on LIF401/404/F01/A01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [8]	DESCRIPTION	LED	SERIAL E2A BIT
MAN [1]	NSA	MN/MN	Manual switch requested on UPSR ring	ABN	42 & 53
MANWKSWBK [1]	NSA	NR/NR	Manual switch back to protected	—	—
MANWKSWPR [1]	NSA	NR/NR	Manual switch of protected path to protecting path	—	—
PATHSEL [1]	SA	CR/CR	Both paths failed, did not switch	—	43
PDI [2]	SA	NR/NR	Payload defect indication	—	—
PLM [2]	SA	MN/MN	Payload label mismatch	—	—
PROTNA [1]	NSA	MN/MN	Protection not available	—	—
RFI [3]	SA	NR/NR	Remote defect indicator	—	—
RFIMM [4]	SA	MN/MN	RDI mismatch	—	—
UNEQ [2]	SA	MN/MN	Path unequipped	—	—
TIM [2]	NSA	MN/MN	Trace identifier message failure	—	—
T-CVP [3]	NSA	NA/NA	Threshold violation for PM STS path BIP errors [5] – NE	—	—
T-CVP [3]	NSA	NA/NA	Threshold violation for PM STS path BIP errors [5] – FE	—	—
T-ESP [3]	NSA	NA/NA	Threshold violation for PM STS path error seconds [5] – NE	—	—
T-ESP [3]	NSA	NA/NA	Threshold violation for PM STS path error seconds [5] – FE	—	—
T-NPJCDET	NSA	NA/NA	Threshold violation for PM STS negative pointer justification count detected [5] – NE	—	—
T-NPJCGEN	NSA	NA/NA	Threshold violation for PM STS negative pointer justification count generated [5] – NE	—	—
T-PPJCDET	NSA	NA/NA	Threshold violation for PM STS positive pointer justification count detected [5] – NE	—	—
T-PPJCGEN	NSA	NA/NA	Threshold violation for PM STS positive pointer justification count generated [5] – NE	—	—
T-PJCSDET	NSA	NA/NA	Threshold violation for PM STS pointer justification count seconds detected [5] – NE		

Table AG. Drop Group: STS Path on LIF401/404/F01/A01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [8]	DESCRIPTION	LED	SERIAL E2A BIT
T-PJCSGEN	NSA	NA/NA	Threshold violation for PM STS pointer justification count generated [5] – NE		
T-PJCDIFF	NSA	NA/NA	Threshold violation for PM STS pointer justification count difference [5] – NE	—	—
T-SESP [3]	NSA	NA/NA	Threshold violation for PM STS path severely errored seconds [5] – NE	—	—
T-SESP [3]	NSA	NA/NA	Threshold violation for PM STS path severely errored seconds [5] – FE	—	—
T-UASP [3]	NSA	NA/NA	Threshold violation for PM STS path unavailable seconds [5] – NE	—	—
T-UASP [3]	NSA	NA/NA	Threshold violation for PM STS path unavailable seconds [5] – FE	—	—
WKSWBK [1]	NSA	NR/NR	Protected path switch back	—	—
WKSWPR [1]	NSA	NR/NR	Switch of protected path to protecting path	—	—
BLSR	—	Event	BLSR ring switch reason	—	—
TIMCHG [2]	—	Event	Trace message identification change	—	—
WTRREVERT [1]	—	Event	Wait to revert time out on UPSR ring (switch reason)	—	—
ERDI-xxx [4][6] where xxx =3 bit RDI	—	Condition	Enhanced remote defect indicator	—	—
PROTECTED-ACT [1]	—	Condition	Protected path is active	—	—
PROTECTING-ACT [1]	—	Condition	Protecting path is active	—	—
PROTECTED-ALL [1]	—	Condition	Protected path conditions (TL1 input only)	—	—
PROTECTING-ALL [1]	—	Condition	Protecting path conditions (TL1 input only)	—	—
PROTECTED-BLSRFAIL [1]	—	Condition	Protected path fails due to BLSR	—	—
PROTECTING-BLSRFAIL [1]	—	Condition	Protecting path fails due to BLSR	—	—
PROTECTED-DG1 [1]	—	Condition	Protected path is Drop Group 1	—	—

Table AG. Drop Group: STS Path on LIF401/404/F01/A01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [8]	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTING-DG1 [1]	—	Condition	Protecting path is Drop Group 1	—	—
PROTECTED-DG2 [1]	—	Condition	Protected path is Drop Group 2	—	—
PROTECTING-DG2 [1]	—	Condition	Protecting path is Drop Group 2	—	—
PROTECTED-DG3 [1]	—	Condition	Protected path is Drop Group 3	—	—
PROTECTING-DG3 [1]	—	Condition	Protecting path is Drop Group 3	—	—
PROTECTED-DG4 [1]	—	Condition	Protected path is Drop Group 4	—	—
PROTECTING-DG4 [1]	—	Condition	Protecting path is Drop Group 4	—	—
PROTECTED-DG1A [1]	—	Condition	Protected path is Drop Group 1A	—	—
PROTECTING-DG1A [1]	—	Condition	Protecting path is Drop Group 1A	—	—
PROTECTED-DG2A [1]	—	Condition	Protected path is Drop Group 2A	—	—
PROTECTING-DG2A [1]	—	Condition	Protecting path is Drop Group 2A	—	—
PROTECTED-DG3A [1]	—	Condition	Protected path is Drop Group 3A	—	—
PROTECTING-DG3A [1]	—	Condition	Protecting path is Drop Group 3A	—	—
PROTECTED-DG4A [1]	—	Condition	Protected path is Drop Group 4A	—	—
PROTECTING-DG4A [1]	—	Condition	Protecting path is Drop Group 4A	—	—
PROTECTED-DG1B [1]	—	Condition	Protected path is Drop Group 1B	—	—
PROTECTING-DG1B [1]	—	Condition	Protecting path is Drop Group 1B	—	—
PROTECTED-DG2B [1]	—	Condition	Protected path is Drop Group 2B	—	—
PROTECTING-DG2B [1]	—	Condition	Protecting path is Drop Group 2B	—	—
PROTECTED-DG3B [1]	—	Condition	Protected path is Drop Group 3B	—	—
PROTECTING-DG3B [1]	—	Condition	Protecting path is Drop Group 3B	—	—
PROTECTED-DG4B [1]	—	Condition	Protected path is Drop Group 4B	—	—

Table AG. Drop Group: STS Path on LIF401/404/F01/A01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [8]	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTING-DG4B [1]	—	Condition	Protecting path is Drop Group 4B	—	—
PROTECTED-FAIL [1]	—	Condition	Protected path is failed	—	—
PROTECTING-FAIL [1]	—	Condition	Protecting path is failed	—	—
PROTECTED-FRCD [1]	—	Condition	Protected path has forced switch	—	—
PROTECTING-FRCD [1]	—	Condition	Protecting path has forced switch	—	—
PROTECTED-LG1 [1]	—	Condition	Protected path is Line Group 1	—	—
PROTECTING-LG1 [1]	—	Condition	Protecting path is Line Group 1	—	—
PROTECTED-LG2 [1]	—	Condition	Protected path is Line Group 2	—	—
PROTECTING-LG2 [1]	—	Condition	Protecting path is Line Group 2	—	—
PROTECTED-LOCKOUT [1]	—	Condition	Lockout switch required on protected path	—	—
PROTECTING-LOCKOUT [1]	—	Condition	Lockout switch required on protecting path	—	—
PROTECTED-MAN [1]	—	Condition	Protected path has manual switch	—	—
PROTECTING-MAN [1]	—	Condition	Protecting path has manual switch	—	—
PROTECTED-RFI [1]	—	Condition	Protected path has RFIP	—	—
PROTECTING-RFI [1]	—	Condition	Protecting path has RFIP	—	—
PROTECTED-STBY [1]	—	Condition	Protected path is standby	—	—
PROTECTING-STBY [1]	—	Condition	Protecting path is standby	—	—
PROTECTED-UNEQ [1]	—	Condition	Protected path is UNEQ (signal label)	—	—
PROTECTING-UNEQ [1]	—	Condition	Protecting path is unequipped (signal label)	—	—
SIGLBL-xxx (RCV) where xxx = 0...255	—	Condition	Received path signal label	—	—
SIGLBL-xxx (TRMT) [7] where xxx = 0...255	—	Condition	Transmit PDI	—	—
Protected−PD1 [1]	—	Condition	Protected path has PDI	—	—
Protecting−PD1 [1]	—	Condition	Protecting path has PDI	—	—

Table AG. Drop Group: STS Path on LIF401/404/F01/A01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [8]	DESCRIPTION	LED	SERIAL E2A BIT
[1] *UPSR ring only.*					
[2] *Applicable only to STS terminated path which carries VT payload.*					
[3] *Applicable only when intermediate STS path enabled or STS path terminated.*					
[4] *Applicable only to LIFA01, LIF404, AND LIFF01.*					
[5] *Either 15-minute or 1-day Threshold Crossing Alert (TCA).*					
[6] *Applicable only when 3-bit RDI is enabled and when intermediate STS path enabled or STS path terminated.*					
[7] *Applicable only when PDI generation is enabled.*					
[8] *Default setting for DUPLEX provisioning shown in table. When the parent equipment is provisioned SIMPLEX, the ACT value is used as the default for both A & B sides.*					

Table AH. Drop Group: STS Path on LIF901

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AISP (TRMT & RCV)	SA	NR	Path alarm indication signal	—	—
BERP-HT	NSA	NA	Bit error ratio high threshold	—	—
BERP-LT	NSA	NA	Bit error ratio low threshold	—	—
ETFAIL	SA	MJ	Extra traffic failed on BLSR ring	—	—
FRCD [1]	NSA	MN	Forced switch requested on UPSR ring	ABN	42 & 53
FRCDWKSWBK [1]	NSA	NR	Protected path forced switch back	—	—
FRCDWKSWPR [1]	NSA	NR	Protected path forced switch to protecting path	—	—
INHPMREPT	NSA	NR	PM reports inhibited	—	—
LOCKOUT [1]	NSA	MN	Lockout requested on UPSR ring	ABN	42 & 53
LOP (RCV & TRMT)	SA	MJ	Loss-of-pointer	—	—
MAN [1]	NSA	MN	Manual switch requested on UPSR ring	ABN	42 & 53
MANWKSWBK [1]	NSA	NR	Manual switch back to protected	—	—
MANWKSWPR [1]	NSA	NR	Manual switch of protected path to protecting path	—	—
PATHSEL [1]	SA	MJ	Both paths failed, did not switch	—	43
PDI (RCV & TRMT)	SA	MN	Path defect indication	—	—

Table AH. Drop Group: STS Path on LIF901 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PLM (RCV & TRMT)	SA	MN	Payload label match failure	—	—
PROTNA [1]	NSA	MN	Protection not available	—	—
RFI (RCV)	SA	NR	Path yellow	—	—
TIM	NSA	MN	Trace identifier message failure	—	—
UNEQ (RCV & TRMT)	SA	MN	Path unequipped	—	—
T-CVP	NSA	NA	Near end path BIP TCA [2]	—	—
T-ESP	NSA	NA	Near end path ES TCA [2]	—	—
T-NPJCGEN	NSA	NA	Negative PJC generated TCA [2]	—	—
T-PPJCGEN	NSA	NA	Positive PJV generated TCA [2]	—	—
T-SESP	NSA	NA	Path SES TCA [2]	—	—
T-UASP	NSA	NA	Path UAS TCA [2]	—	—
WKSWBK [1]	NSA	NR	Protected path switch back	—	—
WKSWPR [1]	NSA	NR	Switch of protected path to protecting path	—	—
BLSR	—	Event	BLSR ring switch reason	—	—
TIMCHG	—	Event	Trace message identifier change	—	—
WTRREVERT [1]	—	Event	Wait to revert time out on UPSR ring (switch reason)	—	—
LCD	—	Condition	Loss of cell delineation	—	—
PROTECTED-ACT [1]	—	Condition	Protected path is active	—	—
PROTECTING-ACT [1]	—	Condition	Protecting path is active	—	—
PROTECTED-ALL [1]	—	Condition	Protected path conditions (TL1 input only)	—	—
PROTECTING-ALL [1]	—	Condition	Protecting path conditions (TL1 input only)	—	—
PROTECTED-BLSRFAIL [1]	—	Condition	Protected path fails due to BLSR	—	—
PROTECTING-BLSRFAIL [1]	—	Condition	Protecting path fails due to BLSR	—	—
PROTECTED-DG1 [1]	—	Condition	Protected path is Drop Group 1	—	—
PROTECTING-DG1 [1]	—	Condition	Protecting path is Drop Group 1	—	—
PROTECTED-DG2 [1]	—	Condition	Protected path is Drop Group 2	—	—
PROTECTING-DG2 [1]	—	Condition	Protecting path is Drop Group 2	—	—
PROTECTED-DG3 [1]	—	Condition	Protected path is Drop Group 3	—	—
PROTECTING-DG3 [1]	—	Condition	Protecting path is Drop Group 3	—	—

Table AH. Drop Group: STS Path on LIF901 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTED-DG4 [1]	—	Condition	Protected path is Drop Group 4	—	—
PROTECTING-DG4 [1]	—	Condition	Protecting path is Drop Group 4	—	—
PROTECTED-DG1A [1]	—	Condition	Protected path is Drop Group 1A	—	—
PROTECTING-DG1A [1]	—	Condition	Protecting path is Drop Group 1A	—	—
PROTECTED-DG2A [1]	—	Condition	Protected path is Drop Group 2A	—	—
PROTECTING-DG2A [1]	—	Condition	Protecting path is Drop Group 2A	—	—
PROTECTED-DG3A [1]	—	Condition	Protected path is Drop Group 3A	—	—
PROTECTING-DG3A [1]	—	Condition	Protecting path is Drop Group 3A	—	—
PROTECTED-DG4A [1]	—	Condition	Protected path is Drop Group 4A	—	—
PROTECTING-DG4A [1]	—	Condition	Protecting path is Drop Group 4A	—	—
PROTECTED-DG1B [1]	—	Condition	Protected path is Drop Group 1B	—	—
PROTECTING-DG1B [1]	—	Condition	Protecting path is Drop Group 1B	—	—
PROTECTED-DG2B [1]	—	Condition	Protected path is Drop Group 2B	—	—
PROTECTING-DG2B [1]	—	Condition	Protecting path is Drop Group 2B	—	—
PROTECTED-DG3B [1]	—	Condition	Protected path is Drop Group 3B	—	—
PROTECTING-DG3B [1]	—	Condition	Protecting path is Drop Group 3B	—	—
PROTECTED-DG4B [1]	—	Condition	Protected path is Drop Group 4B	—	—
PROTECTING-DG4B [1]	—	Condition	Protecting path is Drop Group 4B	—	—
PROTECTED-FAIL [1]	—	Condition	Protected path is failed	—	—
PROTECTING-FAIL [1]	—	Condition	Protecting path is failed	—	—
PROTECTED-FRCD [1]	—	Condition	Protected path has forced switch	—	—
PROTECTING-FRCD [1]	—	Condition	Protecting path has forced switch	—	—
PROTECTED-LG1 [1]	—	Condition	Protected path is Line Group 1	—	—
PROTECTING-LG1 [1]	—	Condition	Protecting path is Line Group 1	—	—
PROTECTED-LG2 [1]	—	Condition	Protected path is Line Group 2	—	—
PROTECTING-LG2 [1]	—	Condition	Protecting path is Line Group 2	—	—

Table AH. Drop Group: STS Path on LIF901 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTED-LOCKOUT [1]	—	Condition	Lockout switch required on protected path	—	—
PROTECTING-LOCKOUT [1]	—	Condition	Lockout switch required on protecting path	—	—
PROTECTED-MAN [1]	—	Condition	Protected path has manual switch	—	—
PROTECTING-MAN [1]	—	Condition	Protecting path has manual switch	—	—
PROTECTED-RFI [1]	—	Condition	Protected path has RFIP	—	—
PROTECTING-RFI [1]	—	Condition	Protecting path has RFIP	—	—
PROTECTED-STBY [1]	—	Condition	Protected path is standby	—	—
PROTECTING-STBY [1]	—	Condition	Protecting path is standby	—	—
PROTECTED-UNEQ [1]	—	Condition	Protected path is UNEQ (signal label)	—	—
PROTECTING-UNEQ [1]	—	Condition	Protecting path is unequipped (signal label)	—	—
SIGLBL-xxx where xxx = 0...255	—	Condition	Path signal label	—	—
Protected−PD1 [1]	—	Condition	Protected path has PD1	—	—
Protecting−PD1 [1]	—	Condition	Protecting path has PD1	—	—

[1] *UPSR ring only.*

[2] *Either 15-minute or 1-day Threshold Crossing Alert (TCA).*

Table AI. Drop Group: STS12c Path on LIFG01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE A/B	DESCRIPTION	LED	SERIAL E2A BIT
AISP (RCV & TRMT)	SA	NR/NR	Path alarm indication signal	—	—
BERP–HT (TRMT)	NSA	NA/NA	Bit error ratio high threshold	—	—
BERP–LT (TRMT)	NSA	NA/NA	Bit error ratio high threshold	—	—
CONCAT	SA	MJ/MJ	Bit error ratio high threshold	—	—
ETFAIL	SA	MJ/MJ	Extra traffic failed on BLSR ring	—	—
FRCD [1]	NSA	MN/MN	Forced switch requested on UPSR ring	ABN	42 & 53
FRCDWKSWBK [1]	NSA	NR/NR	Protected path forced switch back	—	—
FRCDWKSWPR [1]	NSA	NR/NR	Protected path forced switch to protecting path	—	—
INHPMREPT	NSA	NR/NR	PM reports inhibited	—	—
LOCKOUT[1]	NSA	MN/MN	Lockout requested on UPSR ring	ABN	42 & 53
LOP (RCV & TRMT)	SA	MJ/MJ	Loss-of-pointer	—	—
MAN [1]	NSA	MN/MN	Manual switch requested on UPSR ring	ABN	42 & 53
MANWKSWBK [1]	NSA	NR/NR	Manual switch back to protected	—	—
MANWKSWPR [1]	NSA	NR/NR	Manual switch of protected path to protecting path	—	—
PATHSEL [1]	SA	MJ/MJ	Both paths failed, did not switch	—	43
PDI (RCV & TRMT)	SA	MN/MN	Path defect indication	—	—
PLM (RCV & TRMT)	SA	MN/MN	Payload label match failure	—	—
PROTNA [1]	NSA	MN/MN	Protection not available	—	—
RFI	SA	NR/NR	3-bit ERDI payload/server/ connectivity defect	—	—
RFIMM	SA	MN/MN	RDI mismatch	—	—
TIM	NSA	MN/MN	Trace identifier message failure	—	—
UNEQ (RCV & TRMT)	SA	MN/MN	Path unequipped	—	—
T-CVP	NSA	NA/NA	NE/FE path BIP TCA [2]	—	—
T-ESP	NSA	NA/NA	NE/FE path ES TCA [2]	—	—
T-SESP	NSA	NA/NA	NE/FE path SES TCA [2]	—	—
T-UASP	NSA	NA/NA	NE/FE path UAS TCA [2]	—	—
TIMCHG	—	Event	Trace message identifier change	—	—
WKSWBK [1]	NSA	NR/NR	Protected path switch back	—	—
WKSWPR [1]	NSA	NR/NR	Switch of protected path to protecting path	—	—

Table AI. Drop Group: STS12c Path on LIFG01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE A/B	DESCRIPTION	LED	SERIAL E2A BIT
WTRREVERT [1]	—	Event	Wait to revert time out on UPSR ring (switch reason)	—	—
PROTECTED-ACT [1]	—	Condition	Protected path is active	—	—
PROTECTING-ACT [1]	—	Condition	Protecting path is active	—	—
PROTECTED-ALL [1]	—	Condition	Protected path conditions (TL1 input only)	—	—
PROTECTING-ALL [1]	—	Condition	Protecting path conditions (TL1 input only)	—	—
PROTECTED-BLSRFAIL [1]	—	Condition	Protected path fails due to BLSR	—	—
PROTECTING-BLSRFAIL [1]	—	Condition	Protecting path fails due to BLSR	—	—
PROTECTED-DG1 [1]	—	Condition	Protected path is Drop Group 1	—	—
PROTECTING-DG1 [1]	—	Condition	Protecting path is Drop Group 1	—	—
PROTECTED-DG2 [1]	—	Condition	Protected path is Drop¡Group 2	—	—
PROTECTING-DG2 [1]	—	Condition	Protecting path is Drop Group 2	—	—
PROTECTED-DG3 [1]	—	Condition	Protected path is Drop Group 3	—	—
PROTECTING-DG3 [1]	—	Condition	Protecting path is Drop Group 3	—	—
PROTECTED-DG4 [1]	—	Condition	Protected path is Drop Group 4	—	—
PROTECTING-DG4 [1]	—	Condition	Protecting path is Drop Group 4	—	—
PROTECTED-DG1A [1]	—	Condition	Protected path is Drop Group 1A	—	—
PROTECTING-DG1A [1]	—	Condition	Protecting path is Drop Group 1A	—	—
PROTECTED-DG2A [1]	—	Condition	Protected path is Drop¡GroupA 2A	—	—
PROTECTING-DG2A [1]	—	Condition	Protecting path is Drop Group 2A	—	—
PROTECTED-DG3A [1]	—	Condition	Protected path is Drop Group 3A	—	—
PROTECTING-DG3A [1]	—	Condition	Protecting path is Drop Group 3A	—	—
PROTECTED-DG4A [1]	—	Condition	Protected path is Drop Group 4A	—	—
PROTECTING-DG4A [1]	—	Condition	Protecting path is Drop GroupA 4A	—	—
PROTECTED-DG1B [1]	—	Condition	Protected path is Drop Group 1B	—	—
PROTECTING-DG1B [1]	—	Condition	Protecting path is Drop Group 1B	—	—
PROTECTED-DG2B [1]	—	Condition	Protected path is Drop¡Group 2B	—	—

Table AI. Drop Group: STS12c Path on LIFG01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE A/B	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTING-DG2B [1]	—	Condition	Protecting path is Drop Group 2B	—	—
PROTECTED-DG3B [1]	—	Condition	Protected path is Drop Group 3B	—	—
PROTECTING-DG3B [1]	—	Condition	Protecting path is Drop Group 3B	—	—
PROTECTED-DG4B [1]	—	Condition	Protected path is Drop Group 4B	—	—
PROTECTING-DG4B [1]	—	Condition	Protecting path is Drop Group 4B	—	—
PROTECTED-FAIL [1]	—	Condition	Protected path is failed	—	—
PROTECTING-FAIL [1]	—	Condition	Protecting path is failed	—	—
PROTECTED-FRCD [1]	—	Condition	Protected path has forced switch	—	—
PROTECTING-FRCD [1]	—	Condition	Protecting path has forced switch	—	—
PROTECTED-LG1 [1]	—	Condition	Protected path is Line Group 1	—	—
PROTECTING-LG1 [1]	—	Condition	Protecting path is Line Group 1	—	—
PROTECTED-LG2 [1]	—	Condition	Protected path is Line Group 2	—	—
PROTECTING-LG2 [1]	—	Condition	Protecting path is Line Group 2	—	—
PROTECTED-LOCKOUT [1]	—	Condition	Lockout switch request on protected path	—	—
PROTECTING-LOCKOUT [1]	—	Condition	Lockout switch request on protecting path	—	—
PROTECTED-MAN [1]	—	Condition	Protected path has manual switch	—	—
PROTECTING-MAN [1]	—	Condition	Protecting path has manual switch	—	—
PROTECTED-PDI [1]	—	Condition	PDI being received on protected path	—	—
PROTECTING-PDI [1]	—	Condition	PDI being received on protecting path	—	—
PROTECTED-RFI [1]	—	Condition	Protected path has RFIP	—	—
PROTECTING-RFI [1]	—	Condition	Protecting path has RFIP	—	—
PROTECTED-STBY [1]	—	Condition	Protected path is standby	—	—
PROTECTING-STBY [1]	—	Condition	Protecting path is standby	—	—
PROTECTED-UNEQ [1]	—	Condition	Protected path is UNEQ (signal label)	—	—
PROTECTING-UNEQ[1]	—	Condition	Protecting path is UNEQ (signal label)	—	—
SIGLBL-xxx where xxx = 0...255	—	Condition	Path signal label	—	—

Table AI. Drop Group: STS12c Path on LIFG01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE A/B	DESCRIPTION	LED	SERIAL E2A BIT
ERDI	—	Condition	Enhanced remote defect indicator	—	—
Protected–PDI [1]	—	Condition	Protected path has PD1	—	—
Protecting–PDI [1]	—	Condition	Protecting path has PD1	—	—
[1] *UPSR ring only.* [2] *Either 15-minutes or 1-day Threshold Crossing Alert (TCA)*					

Table AJ. Drop Group: VT Path on DMI102/301

ALARM CONDITON	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AISP (RCV & TRMT)	SA	NR	VT path AIS	—	—
BERP-HT	NSA	NA	Bit error ratio high threshold	—	—
BERP-LT	NSA	NA	Bit error ratio low threshold	—	—
FRCD [1]	NSA	MN	Forced switch requested on UPSR ring	ABN	42 & 53
FRCDWKSWBK [1]	NSA	NR	Protected path forced switch back	—	—
FRCDWKSWPR [1]	NSA	NR	Protected path forced switch to protecting path	—	—
INHPMREPT	NSA	NR	All scheduled PM reports inhibited	—	—
LOCKOUT [1]	NSA	MN	Lockout requested on UPSR ring	ABN	42 & 53
LOP (RCV & TRMT)	SA	MN	VT loss-of-pointer	—	—
MAN [1]	NSA	MN	Manual switch requested on UPSR ring	ABN	42 & 53
MANWKSWBK [1]	NSA	NR	Manual switch back to protected	—	—
MANWKSWPR [1]	NSA	NR	Manual switch of protected path to protecting path	—	—
PATHSEL [1]	SA	MJ	Both paths failed, did not switch	—	43
PLM (RCV & TRMT)	SA	MN	Payload label mismatch	—	—
PROTNA [1]	NSA	MN	Protection not available	—	—
RFI (RCV & TRMT)	SA	NR	VT path yellow	—	—
T-CVP	NSA	NA	Threshold violation for PM VT path BIP errors [2] – NE	—	—
T-CVP	NSA	NA	Threshold violation for PM VT path BIP errors [2] – FE	—	—

Table AJ. Drop Group: VT Path on DMI102/301 (cont)

ALARM CONDITON	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
T-ESP	NSA	NA	Threshold violation for PM VT path error seconds [2] – NE	—	—
T-ESP	NSA	NA	Threshold violation for PM VT path error seconds [2] – FE	—	—
T-NPJCGEN	NSA	NA	Threshold violation for PM VT negative pointer justification count generated [2]	—	—
T-PPJCGEN	NSA	NA	Threshold violation for PM VT positive pointer justification count generated [2]	—	—
T-SESP	NSA	NA	Threshold violation for PM VT path severely errored seconds [2] – NE	—	—
T-SESP	NSA	NA	Threshold violation for PM VT path severely errored seconds [2] – FE	—	—
T-UASP	NSA	NA	Threshold violation for PM VT path unavailable seconds [2] – NE	—	—
T-UASP	NSA	NA	Threshold violation for PM VT path unavailable seconds [2] – FE	—	—
UNEQ (RCV & TRMT)	SA	MN	Path unequipped	—	—
VTSIZE	SA	MN	VT size mismatch	—	—
WKSWBK [1]	NSA	NR	Protected path switch back	—	—
WKSWPR [1]	NSA	NR	Switch of protected path to protecting path	—	—
PROTECTED-ACT [1]	—	Condition	Protected path is active	—	—
PROTECTING-ACT [1]	—	Condition	Protecting path is active	—	—
PROTECTED-ALL [1]	—	Condition	Protected path conditions (TL1 input only)	—	—
PROTECTING-ALL [1]	—	Condition	Protecting path conditions (TL1 input only)	—	—
PROTECTED-DG1 [1]	—	Condition	Protected path is Drop Group 1	—	—
PROTECTING-DG1 [1]	—	Condition	Protecting path is Drop Group 1	—	—
PROTECTED-DG2 [1]	—	Condition	Protected path is Drop Group 2	—	—
PROTECTING-DG2 [1]	—	Condition	Protecting path is Drop Group 2	—	—
PROTECTED-DG3 [1]	—	Condition	Protected path is Drop Group 3	—	—
PROTECTING-DG3 [1]	—	Condition	Protecting path is Drop Group 3	—	—
PROTECTED-DG4 [1]	—	Condition	Protected path is Drop Group 4	—	—
PROTECTING-DG4 [1]	—	Condition	Protecting path is Drop Group 4	—	—

Table AJ. Drop Group: VT Path on DMI102/301 (cont)

ALARM CONDITON	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTED-DG1A [1]	—	Condition	Protected path is Drop Group 1A	—	—
PROTECTING-DG1A [1]	—	Condition	Protecting path is Drop Group 1A	—	—
PROTECTED-DG2A [1]	—	Condition	Protected path is Drop Group 2A	—	—
PROTECTING-DG2A [1]	—	Condition	Protecting path is Drop Group 2A	—	—
PROTECTED-DG3A [1]	—	Condition	Protected path is Drop Group 3A	—	—
PROTECTING-DG3A [1]	—	Condition	Protecting path is Drop Group 3A	—	—
PROTECTED-DG4A [1]	—	Condition	Protected path is Drop Group 4A	—	—
PROTECTING-DG4A [1]	—	Condition	Protecting path is Drop Group 4A	—	—
PROTECTED-DG1B [1]	—	Condition	Protected path is Drop Group 1B	—	—
PROTECTING-DG1B [1]	—	Condition	Protecting path is Drop Group 1B	—	—
PROTECTED-DG2B [1]	—	Condition	Protected path is Drop Group 2B	—	—
PROTECTING-DG2B [1]	—	Condition	Protecting path is Drop Group 2B	—	—
PROTECTED-DG3B [1]	—	Condition	Protected path is Drop Group 3B	—	—
PROTECTING-DG3B [1]	—	Condition	Protecting path is Drop Group 3B	—	—
PROTECTED-DG4B [1]	—	Condition	Protected path is Drop Group 4B	—	—
PROTECTING-DG4B [1]	—	Condition	Protecting path is Drop Group 4B	—	—
PROTECTED-FAIL [1]	—	Condition	Protected path is failed	—	—
PROTECTING-FAIL [1]	—	Condition	Protecting path is failed	—	—
PROTECTED-FRCD [1]	—	Condition	Protected path has forced switch	—	—
PROTECTING-FRCD [1]	—	Condition	Protecting path has forced switch	—	—
PROTECTED-LG1 [1]	—	Condition	Protected path is Line Group 1	—	—
PROTECTING-LG1 [1]	—	Condition	Protecting path is Line Group 1	—	—
PROTECTED-LG2 [1]	—	Condition	Protected path is Line Group 2	—	—
PROTECTING-LG2 [1]	—	Condition	Protecting path is Line Group 2	—	—
PROTECTED-LOCKOUT [1]	—	Condition	Lockout switch required on protected path	—	—

Table AJ. Drop Group: VT Path on DMI102/301

ALARM CONDITON	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTING-LOCKOUT [1]	—	Condition	Lockout switch required on protecting path	—	—
PROTECTED-MAN [1]	—	Condition	Protected path has manual switch	—	—
PROTECTING-MAN [1]	—	Condition	Protecting path has manual switch	—	—
PROTECTED-RFI [1]	—	Condition	Protected path has RFIP	—	—
PROTECTING-RFI [1]	—	Condition	Protecting path has RFIP	—	—
PROTECTED-STBY [1]	—	Condition	Protected path is standby	—	—
PROTECTING-STBY [1]	—	Condition	Protecting path is standby	—	—
PROTECTED-UNEQ [1]	—	Condition	Protected path is UNEQ (signal label)	—	—
PROTECTING-UNEQ [1]	—	Condition	Protecting path is unequipped (signal label)	—	—
SIGLBL-( )	—	Condition	Signal label with ( ) code	—	—
TSA-n where: n = MONE, MONF, SPLTA, SPLTB, SPLTE, SPLTF, LOOPE, LOOPF	—	Condition	Test access mode	—	—
TSN-n where: n = 1...999	—	Condition	Test session number n is active	—	—

[1] *UPSR ring only.*

[2] *Either 15-minute or 1-day Threshold Crossing Alert (TCA)*

Table AK. Drop Group: VT Path on LIF201/501/701/D01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AISP	SA	NR	Path alarm indication signal detected	—	—
BERP-HT	NSA	NA	Bit error ratio high threshold	—	—
BERP-LT	NSA	NA	Bit error ratio low threshold	—	—
FRCD [1]	NSA	MN	Forced switch requested on UPSR ring	ABN	42 & 53
FRCDWKSWBK [1]	NSA	NR	Protected path forced switch back	—	—
FRCDWKSWPR [1]	NSA	NR	Protected path forced switch to protecting path	—	—

Table AK. Drop Group: VT Path on LIF201/501/701/D01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
INHPMREPT	NSA	NR	All scheduled PM reports inhibited	—	—
LOCKOUT [1]	NSA	MN	Lockout requested on UPSR ring	ABN	42 & 53
LOP	SA	MJ	VT loss-of-pointer	—	—
MAN [1]	NSA	MN	Manual switch requested on UPSR ring	ABN	42 & 53
MANWKSWBK [1]	NSA	NR	Manual switch back to protected	—	—
MANWKSWPR [1]	NSA	NR	Manual switch of protected path to protecting path	—	—
PATHSEL [1]	SA	MJ	Both paths failed, did not switch	—	43
PLM	SA	MN	Receive VT payload label mismatch	—	—
PROTNA [1]	NSA	MN	Protection not available	—	—
T-NPJCDET	NSA	NA	Threshold violation for PM VT negative pointer justification count detected [2] – NE	—	—
T-NPJCGEN [3]	NSA	NA	Threshold violation for PM VT negative pointer justification count generated [2] – NE	—	—
T-PPJCDET	NSA	NA	Threshold violation for PM VT positive pointer justification count detected [2] – NE	—	—
T-PPJCGEN [3]	NSA	NA	Threshold violation for PM VT positive pointer justification count generated [2] – NE	—	—
T-PJCSDET [3]	NSA	NA	Threshold violation for PM VT pointer justification count seconds detected [2] – NE		
T-PJCSGEN [3]	NSA	NA	Threshold violation for PM VT pointer justification count generated [2] – NE		
T-PJCDIFF [3]	NSA	NA	Threshold violation for PM VT pointer justification count difference [2] – NE	—	—
UNEQ	SA	MN	Receive VT path unequipped	—	—
VTSIZE	SA	MJ	VT size mismatch	—	—
WKSWBK [1]	NSA	NR	Protected path switch back	—	—
WKSWPR [1]	NSA	NR	Switch of protected path to protecting path	—	—

Table AK. Drop Group: VT Path on LIF201/501/701/D01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
WTRREVERT [1]	—	Event	Wait to revert time out (switch reason) on UPSR ring	—	—
PROTECTED-ACT [1]	—	Condition	Protected path is active	—	—
PROTECTING-ACT [1]	—	Condition	Protecting path is active	—	—
PROTECTED-ALL [1]	—	Condition	Protected path conditions (TL1 input only)	—	—
PROTECTING-ALL [1]	—	Condition	Protecting path conditions (TL1 input only)	—	—
PROTECTED-DG1 [1]	—	Condition	Protected path is Drop Group 1	—	—
PROTECTING-DG1 [1]	—	Condition	Protecting path is Drop Group 1	—	—
PROTECTED-DG2 [1]	—	Condition	Protected path is Drop Group 2	—	—
PROTECTING-DG2 [1]	—	Condition	Protecting path is Drop Group 2	—	—
PROTECTED-DG3 [1]	—	Condition	Protected path is Drop Group 3	—	—
PROTECTING-DG3 [1]	—	Condition	Protecting path is Drop Group 3	—	—
PROTECTED-DG4 [1]	—	Condition	Protected path is Drop Group 4	—	—
PROTECTING-DG4 [1]	—	Condition	Protecting path is Drop Group 4	—	—
PROTECTED-DG1A [1]	—	Condition	Protected path is Drop Group 1A	—	—
PROTECTING-DG1A [1]	—	Condition	Protecting path is Drop Group 1A	—	—
PROTECTED-DG2A [1]	—	Condition	Protected path is Drop Group 2A	—	—
PROTECTING-DG2A [1]	—	Condition	Protecting path is Drop Group 2A	—	—
PROTECTED-DG3A [1]	—	Condition	Protected path is Drop Group 3A	—	—
PROTECTING-DG3A [1]	—	Condition	Protecting path is Drop Group 3A	—	—
PROTECTED-DG4A [1]	—	Condition	Protected path is Drop Group 4A	—	—
PROTECTING-DG4A [1]	—	Condition	Protecting path is Drop Group 4A	—	—
PROTECTED-DG1B [1]	—	Condition	Protected path is Drop Group 1B	—	—
PROTECTING-DG1B [1]	—	Condition	Protecting path is Drop Group 1B	—	—
PROTECTED-DG2B [1]	—	Condition	Protected path is Drop Group 2B	—	—
PROTECTING-DG2B [1]	—	Condition	Protecting path is Drop Group 2B	—	—
PROTECTED-DG3B [1]	—	Condition	Protected path is Drop Group 3B	—	—
PROTECTING-DG3B [1]	—	Condition	Protecting path is Drop Group 3B	—	—

Table AK. Drop Group: VT Path on LIF201/501/701/D01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTED-DG4B [1]	—	Condition	Protected path is Drop Group 4B	—	—
PROTECTING-DG4B [1]	—	Condition	Protecting path is Drop Group 4B	—	—
PROTECTED-FAIL [1]	—	Condition	Protected path is failed	—	—
PROTECTING-FAIL [1]	—	Condition	Protecting path is failed	—	—
PROTECTED-FRCD [1]	—	Condition	Protected path has forced switch	—	—
PROTECTING-FRCD [1]	—	Condition	Protecting path has forced switch	—	—
PROTECTED-LG1 [1]	—	Condition	Protected path is Line Group 1	—	—
PROTECTING-LG1 [1]	—	Condition	Protecting path is Line Group 1	—	—
PROTECTED-LG2 [1]	—	Condition	Protected path is Line Group 2	—	—
PROTECTING-LG2 [1]	—	Condition	Protecting path is Line Group 2	—	—
PROTECTED-LOCKOUT [1]	—	Condition	Lockout switch required on protected path	—	—
PROTECTING-LOCKOUT [1]	—	Condition	Lockout switch required on protecting path	—	—
PROTECTED-MAN [1]	—	Condition	Protected path has manual switch	—	—
PROTECTING-MAN [1]	—	Condition	Protecting path has manual switch	—	—
PROTECTED-RFI [1]	—	Condition	Protected path has RFIP	—	—
PROTECTING-RFI [1]	—	Condition	Protecting path has RFIP	—	—
PROTECTED-STBY [1]	—	Condition	Protected path is standby	—	—
PROTECTING-STBY [1]	—	Condition	Protecting path is standby	—	—
PROTECTED-UNEQ [1]	—	Condition	Protected path is UNEQ (signal label)	—	—
PROTECTING-UNEQ [1]	—	Condition	Protecting path is unequipped (signal label)	—	—
TSA-n where: n = MONE, MONF, SPLTA, SPLTB, SPLTE, SPLTF, LOOPE, LOOPF	—	Condition	Test access mode	—	—
TSN-n where: n = 1...999	—	Condition	Test session number *n* is active	—	—

[1] *UPSR ring only.*

[2] *Either 15-minute or 1-day Threshold Crossing Alert (TCA).*

[3] *Does not apply to LIF201*

Table AL. Drop Group: VT Path on LIF401/404/F01/A01

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [4]	DESCRIPTION	LED	SERIAL E2A BIT
AISP	SA	NR/NR	Path alarm indication signal detected	—	—
BERP-HT	NSA	NA/NA	Bit error ratio high threshold	—	—
BERP-LT	NSA	NA/NA	Bit error ratio low threshold	—	—
FRCD [1]	NSA	MN/MN	Forced switch requested on UPSR ring	ABN	42 & 53
FRCDWKSWBK [1]	NSA	NR/NR	Protected path forced switch back	—	—
FRCDWKSWPR [1]	NSA	NR/NR	Protected path forced switch to protecting path	—	—
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
LOCKOUT [1]	NSA	MN/MN	Lockout requested on UPSR ring	ABN	42 & 53
LOP	SA	MJ/MN	VT loss-of-pointer	—	—
MAN [1]	NSA	MN/MN	Manual switch requested on UPSR ring	ABN	42 & 53
MANWKSWBK [1]	NSA	NR/NR	Manual switch back to protected	—	—
MANWKSWPR [1]	NSA	NR/NR	Manual switch of protected path to protecting path	—	—
PATHSEL [1]	SA	MJ/MJ	Both paths failed, did not switch	—	43
PLM	SA	MN/MN	Receive payload label mismatch failure	—	—
PROTNA [1]	NSA	MN/MN	Protection not available	—	—
T-NPJCDET [2]	NSA	NA/NA	Threshold violation for PM VT negative pointer justification count detected [3] – NE	—	—
T-NPJCGEN [2]	NSA	NA/NA	Threshold violation for PM VT negative pointer justification countgenerated [3] – NE	—	—
T-PPJCDET [2]	NSA	NA/NA	Threshold violation for PM VT positive pointer justification countdetected [3] – NE	—	—
T-PPJCGEN [2]	NSA	NA/NA	Threshold violation for PM VT positive pointer justification count generated [3] – NE	—	—

Table AL. Drop Group: VT Path on LIF401/404/F01/A01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [4]	DESCRIPTION	LED	SERIAL E2A BIT
T-PJCSDET [2]	NSA	NA/NA	Threshold violation for PM VT pointer justification count seconds detected [3] – NE		
T-PJCSGEN [2]	NSA	NA/NA	Threshold violation for PM VT pointer justification count generated [3] – NE		
T-PJCDIFF [2]	NSA	NA/NA	Threshold violation for PM VT pointer justification count difference [3] – NE	—	—
UNEQ	SA	MN/MN	Receive path unequipped	—	—
VTSIZE	SA	MJ/MN	VT size mismatch	—	—
WKSWBK [1]	NSA	NR/NR	Protected path switch back	—	—
WKSWPR [1]	NSA	NR/NR	Switch of protected path to protecting path	—	—
WTRREVERT [1]	—	Event	Wait to revert time out (switch reason) on UPSR ring	—	—
PROTECTED-ACT [1]	—	Condition	Protected path is active	—	—
PROTECTING-ACT [1]	—	Condition	Protecting path is active	—	—
PROTECTED-ALL [1]	—	Condition	Protected path conditions (TL1 input only)	—	—
PROTECTING-ALL [1]	—	Condition	Protecting path conditions (TL1 input only)	—	—
PROTECTED-DG1 [1]	—	Condition	Protected path is Drop Group 1	—	—
PROTECTING-DG1 [1]	—	Condition	Protecting path is Drop Group 1	—	—
PROTECTED-DG2 [1]	—	Condition	Protected path is Drop Group 2	—	—
PROTECTING-DG2 [1]	—	Condition	Protecting path is Drop Group 2	—	—
PROTECTED-DG3 [1]	—	Condition	Protected path is Drop Group 3	—	—
PROTECTING-DG3 [1]	—	Condition	Protecting path is Drop Group 3	—	—
PROTECTED-DG4 [1]	—	Condition	Protected path is Drop Group 4	—	—
PROTECTING-DG4 [1]	—	Condition	Protecting path is Drop Group 4	—	—
PROTECTED-DG1A [1]	—	Condition	Protected path is Drop Group 1A	—	—
PROTECTING-DG1A [1]	—	Condition	Protecting path is Drop Group 1A	—	—
PROTECTED-DG2A [1]	—	Condition	Protected path is Drop Group 2A	—	—

Table AL. Drop Group: VT Path on LIF401/404/F01/A01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [4]	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTING-DG2A [1]	—	Condition	Protecting path is Drop Group 2A	—	—
PROTECTED-DG3A [1]	—	Condition	Protected path is Drop Group 3A	—	—
PROTECTING-DG3A [1]	—	Condition	Protecting path is Drop Group 3A	—	—
PROTECTED-DG4A [1]	—	Condition	Protected path is Drop Group 4A	—	—
PROTECTING-DG4A [1]	—	Condition	Protecting path is Drop Group 4A	—	—
PROTECTED-DG1B [1]	—	Condition	Protected path is Drop Group 1B	—	—
PROTECTING-DG1B [1]	—	Condition	Protecting path is Drop Group 1B	—	—
PROTECTED-DG2B [1]	—	Condition	Protected path is Drop Group 2B	—	—
PROTECTING-DG2B [1]	—	Condition	Protecting path is Drop Group 2B	—	—
PROTECTED-DG3B [1]	—	Condition	Protected path is Drop Group 3B	—	—
PROTECTING-DG3B [1]	—	Condition	Protecting path is Drop Group 3B	—	—
PROTECTED-DG4B [1]	—	Condition	Protected path is Drop Group 4B	—	—
PROTECTING-DG4B [1]	—	Condition	Protecting path is Drop Group 4B	—	—
PROTECTED-FAIL [1]	—	Condition	Protected path is failed	—	—
PROTECTING-FAIL [1]	—	Condition	Protecting path is failed	—	—
PROTECTED-FRCD [1]	—	Condition	Protected path has forced switch	—	—
PROTECTING-FRCD [1]	—	Condition	Protecting path has forced switch	—	—
PROTECTED-LG1 [1]	—	Condition	Protected path is Line Group 1	—	—
PROTECTING-LG1 [1]	—	Condition	Protecting path is Line Group 1	—	—
PROTECTED-LG2 [1]	—	Condition	Protected path is Line Group 2	—	—
PROTECTING-LG2 [1]	—	Condition	Protecting path is Line Group 2	—	—
PROTECTED-LOCKOUT [1]	—	Condition	Lockout switch required on protected path	—	—

Table AL. Drop Group: VT Path on LIF401/404/F01/A01 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY [4]	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTING-LOCKOUT [1]	—	Condition	Lockout switch required on protecting path	—	—
PROTECTED-MAN [1]	—	Condition	Protected path has manual switch	—	—
PROTECTING-MAN [1]	—	Condition	Protecting path has manual switch	—	—
PROTECTED-RFI [1]	—	Condition	Protected path has RFIP	—	—
PROTECTING-RFI [1]	—	Condition	Protecting path has RFIP	—	—
PROTECTED-STBY [1]	—	Condition	Protected path is standby	—	—
PROTECTING-STBY [1]	—	Condition	Protecting path is standby	—	—
PROTECTED-UNEQ [1]	—	Condition	Protected path is UNEQ (signal label)	—	—
PROTECTING-UNEQ [1]	—	Condition	Protecting path is unequipped (signal label)	—	—
TSA-n where: n = MONE, MONF, SPLTA, SPLTB, SPLTE, SPLTF, LOOPE, LOOPF	—	Condition	Test access mode	—	—
TSN-n where: n = 1...999	—	Condition	Test session number n is active	—	—

[1] *UPSR ring only.*

[2] *Reported only against the selected VT.*

[3] *Either 15-minutes or 1-day Threshold Crossing Alert (TCA).*

[4] *Default setting for DUPLEX provisioning shown in table. When the parent equipment is provisioned SIMPLEX, the ACT value is used as the default for both A & B sides.*

Table AM. Drop Group: VT Path on LIF601

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE	DESCRIPTION	LED	SERIAL E2A BIT
AISP	SA	NR	Path alarm indication signal detected	—	—
FRCDWKSWBK [1]	NSA	NR	Protected path forced switch back	—	—
FRCDWKSWPR [1]	NSA	NR	Protected path forced switch to protecting path	—	—
INHPMREPT	NSA	NR	All scheduled PM reports inhibited	—	—
LOP	SA	MN	VT loss-of-pointer	—	—
MANWKSWBK [1]	NSA	NR	Manual switch back to protected	—	—
MANWKSWPR [1]	NSA	NR	Manual switch of protected path to protecting path	—	—
PATHSEL [1]	SA	MJ	Both paths failed, did not switch	—	43
PLM	SA	MN	Payload label mismatch	—	—
PROTNA [1]	NSA	MN	Protection not available	—	—
RFI	SA	NR	VT path yellow	—	—
T-CVP	NSA	NA	Threshold violation for PM VT path BIP errors [2] – NE	—	—
T-CVP	NSA	NA	Threshold violation for PM VT path BIP errors [2] – FE	—	—
T-ESP	NSA	NA	Threshold violation for PM VT path error seconds [2] – NE	—	—
T-ESP	NSA	NA	Threshold violation for PM VT path error seconds [2] – FE	—	—
T-NPJCGEN	NSA	NA	Threshold violation for PM VT negative pointer justification count generated [2]	—	—
T-PPJCGEN	NSA	NA	Threshold violation for PM VT positive pointer justification count generated [2]	—	—
T-SESP	NSA	NA	Threshold violation for PM VT path severely errored seconds [2] – NE	—	—
T-SESP	NSA	NA	Threshold violation for PM VT path severely errored seconds [2] – FE	—	—
T-UASP	NSA	NA	Threshold violation for PM VT path unavailable seconds [2] – NE	—	—

Table AM. Drop Group: VT Path on LIF601 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE	DESCRIPTION	LED	SERIAL E2A BIT
T-UASP	NSA	NA	Threshold violation for PM VT path unavailable seconds [2] – FE	—	—
UNEQ	SA	MN	Path unequipped	—	—
VTSIZE	SA	MN	VT size mismatch	—	—
WKSWBK [1]	NSA	NR	Protected path switch back	—	—
WKSWPR [1]	NSA	NR	Switch of protected path to protecting path	—	—
PROTECTED-ACT [1]	—	Condition	Protected path is active	—	—
PROTECTING-ACT [1]	—	Condition	Protecting path is active	—	—
PROTECTED-ALL [1]	—	Condition	Protected path conditions (TL1 input only)	—	—
PROTECTING-ALL [1]	—	Condition	Protecting path conditions (TL1 input only)	—	—
PROTECTED-DG1 [1]	—	Condition	Protected path is Drop Group 1	—	—
PROTECTING-DG1 [1]	—	Condition	Protecting path is Drop Group 1	—	—
PROTECTED-DG2 [1]	—	Condition	Protected path is Drop Group 2	—	—
PROTECTING-DG2 [1]	—	Condition	Protecting path is Drop Group 2	—	—
PROTECTED-DG3 [1]	—	Condition	Protected path is Drop Group 3	—	—
PROTECTING-DG3 [1]	—	Condition	Protecting path is Drop Group 3	—	—
PROTECTED-DG4 [1]	—	Condition	Protected path is Drop Group 4	—	—
PROTECTING-DG4 [1]	—	Condition	Protecting path is Drop Group 4	—	—
PROTECTED-DG1A [1]	—	Condition	Protected path is Drop Group 1A	—	—
PROTECTING-DG1A [1]	—	Condition	Protecting path is Drop Group 1A	—	—
PROTECTED-DG2A [1]	—	Condition	Protected path is Drop Group 2A	—	—
PROTECTING-DG2A [1]	—	Condition	Protecting path is Drop Group 2A	—	—
PROTECTED-DG3A [1]	—	Condition	Protected path is Drop Group 3A	—	—
PROTECTING-DG3A [1]	—	Condition	Protecting path is Drop Group 3A	—	—
PROTECTED-DG4A [1]	—	Condition	Protected path is Drop Group 4A	—	—
PROTECTING-DG4A [1]	—	Condition	Protecting path is Drop Group 4A	—	—

Table AM. Drop Group: VT Path on LIF601 (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTED-DG1B [1]	—	Condition	Protected path is Drop Group 1B	—	—
PROTECTING-DG1B [1]	—	Condition	Protecting path is Drop Group 1B	—	—
PROTECTED-DG2B [1]	—	Condition	Protected path is Drop Group 2B	—	—
PROTECTING-DG2B [1]	—	Condition	Protecting path is Drop Group 2B	—	—
PROTECTED-DG3B [1]	—	Condition	Protected path is Drop Group 3B	—	—
PROTECTING-DG3B [1]	—	Condition	Protecting path is Drop Group 3B	—	—
PROTECTED-DG4B [1]	—	Condition	Protected path is Drop Group 4B	—	—
PROTECTING-DG4B [1]	—	Condition	Protecting path is Drop Group 4B	—	—
PROTECTED-FAIL [1]	—	Condition	Protected path is failed	—	—
PROTECTING-FAIL [1]	—	Condition	Protecting path is failed	—	—
PROTECTED-FRCD [1]	—	Condition	Protected path has forced switch	—	—
PROTECTING-FRCD [1]	—	Condition	Protecting path has forced switch	—	—
PROTECTED-LG1 [1]	—	Condition	Protected path is Line Group 1	—	—
PROTECTING-LG1 [1]	—	Condition	Protecting path is Line Group 1	—	—
PROTECTED-LG2 [1]	—	Condition	Protected path is Line Group 2	—	—
PROTECTING-LG2 [1]	—	Condition	Protecting path is Line Group 2	—	—
PROTECTED-LOCKOUT [1]	—	Condition	Lockout switch required on protected path	—	—
PROTECTING-LOCKOUT [1]	—	Condition	Lockout switch required on protecting path	—	—
PROTECTED-MAN [1]	—	Condition	Protected path has manual switch	—	—
PROTECTING-MAN [1]	—	Condition	Protecting path has manual switch	—	—
PROTECTED-RFI [1]	—	Condition	Protected path has RFIP	—	—
PROTECTING-RFI [1]	—	Condition	Protecting path has RFIP	—	—
PROTECTED-STBY [1]	—	Condition	Protected path is standby	—	—
PROTECTING-STBY [1]	—	Condition	Protecting path is standby	—	—
PROTECTED-UNEQ [1]	—	Condition	Protected path is UNEQ (signal label)	—	—

Table AM. Drop Group: VT Path on LIF601

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE	DESCRIPTION	LED	SERIAL E2A BIT
PROTECTING-UNEQ [1]	—	Condition	Protecting path is unequipped (signal label)	—	—
SIGLBL-( )	—	Condition	Signal label equipped with ( ) code	—	—
TSA-n where: n = MONE, MONF, SPLTA, SPLTB, SPLTE, SPLTF, LOOPE, LOOPF	—	Condition	Test access mode	—	—
TSN-n where: n = 1...999	—	Condition	Test session number *n* is active	—	—

[1] *UPSR ring only.*

[2] *Either 15-minutes or 1-day Threshold Crossing Alert (TCA).*

Table AN. Adaptation Layer 5 (AAL5)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
INHPMREPTQOS	NSA	NR	QOS PM report inhibited	—	—
T-PTCOLERR	NSA	NA	Protocol error TCA*	—	—
T-TXERR	NSA	NA	Transfer error TCA*	—	—
T-DISAAL5FR	NSA	NA	Received frames discarded – no buffer available TCA*	—	—
T-DISRFCHDR	NSA	NA	Received frames discarded – RFC1483 header TCA*	—	—

* *Either 15-minutes or 1-day Threshold Crossing Alert (TCA).*

Table AO. ATM Port

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
INCOMPATGFC	NSA	MJ	Incompatible GFC protocol	—	—
INHPMREPTNDC	NSA	NR	Scheduled ATMPORT NDC reports inhibited	—	—
INHPMREPTQOS	NSA	NR	Scheduled ATMPORT QOS PM reports inhibited	—	—
LCD (RX)	SA	MJ	Loss of cell delineation	—	—
T-CDHEC	NSA	NA	Bad HEC cells discarded TCA*	—	—
T-CDHDRVP	NSA	NA	Header error cells discarded TCA*	—	—
* *Either 15-minutes or 1-day Threshold Crossing Alert (TCA).*					

Table AP. ATM Processor

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
INHPMREPTNDC	NSA	NR	Scheduled NDC reports inhibited	—	—
INHPMREPTNTM	NSA	NR	Scheduled NTM reports inhibited	—	—
INHPMREPTQOS	NSA	NR	Scheduled QOS PM reports inhibited	—	—
T-CDCR10	NSA	NA	CRC10 errored cells TCA*	—	—
T-CDINVLD	NSA	NA	Invalid cells TCA*	—	—
T-CDCONG0+1	NSA	NA	Congestion discard CLP=0+1 cells TCA* – 5 minutes	—	—
T-CDCONGPROC	NSA	NA	Discard by OAM processor TCA* – 5 minutes	—	—
* *Either 15-minutes or 1-day Threshold Crossing Alert (TCA).*					

Table AQ. Bidirectional Line-Switched Ring (BLSR)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
BLSRCONN-LG1	NSA	MN	Internode communication lost to NE on Line Group 1	—	—
BLSRCONN-LG2	NSA	MN	Internode communication lost to NE on Line Group 2	—	—
BLSRPROV-LG1	NSA	MN	NE on Line Group 1 is not set to BLSR mode or auto map	—	—
BLSRPROV-LG2	NSA	MN	NE on Linge Group 2 is not set to BLSR mode or auto map	—	—
BLSROUTOFSYNC	NSA	MN	BLSR map is out of sync	—	—
DUPNODEID	NSA	MN	Duplicate Node ID	—	—
RINGMAPPROV	NSA	MN	Ring map misprovisioning (broken ring)	—	—
RINGXCONNPROV	NSA	MN	Cross-connect map misprovisioning	—	—
RINGBLSRALM	NSA	MN	BLSR ring alarm	—	—
BLSRMULTIFLT	NSA	MJ	BLSR multi-ring faults (node isolated)	—	—
KSTATE	—	Condition	K byte state (TL1 input only)	—	—
KSTATE-xxx [1]	—	Condition	K byte state (TL1 output only)	—	—
LG1SWPRIORITY	—	Condition	Line Group 1 switch priority at near end or far end (TL1 input only)	—	—
LG1SWPRIORITY-yyy [2]	—	Condition	Line Group 1 switch priority at near end or far end (TL1 output only)	—	—
LG2SWPRIORITY	—	Condition	Line Group 2 switch priority at near end or far end (TL1 input only)	—	—
LG2SWPRIORITY-yyy [2]	—	Condition	Line Group 2 switch priority at near end or far end (TL1 output only)	—	—

[1] *Where xxx = IDLE (K byte state idle), SWITCHING (K byte state switching), PASSTHRU_UNI (K byte state Passthru Unidirectional Full), PASSTHRU_BI (K byte state Passthru Bidirectional Full), or PASSTHRU_KBYTE (K byte state Passthru Kbyte).*

[2] *Where yyy = IDLE (Idle), WTR (Wait to Restore), MAN (Manual Switch Request), SIGDEG (Signal Degraded), SIGFAIL (Signal Failed), FRCD (Forced Switch Request), LPS (Lockout – Entire Ring), or LOWR (Lockout – Local NE).*

Table AR. BITS Synchronization Sources

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
( )-DG1A-n* where: n = 1...4	NSA	MN/MN	Drop group 1, side A reference fail	—	17
( )-DG1B-n* where: n = 1...4	NSA	MN/MN	Drop group 1, side B reference fail	—	17
( )-DG2A-n* where: n = 1...4	NSA	MN/MN	Drop group 2, side A reference fail	—	17
( )-DG2B-n* where: n = 1...4	NSA	MN/MN	Drop group 2, side B reference fail	—	17
( )-DG3A-n* where: n = 1...4	NSA	MN/MN	Drop group 3, side A reference fail	—	17
( )-DG3B-n* where: n = 1...4	NSA	MN/MN	Drop group 3, side B reference fail	—	17
( )-DG4A-n* where: n = 1...4	NSA	MN/MN	Drop group 4, side A reference fail	—	17
( )-DG4B-n* where: n = 1...4	NSA	MN/MN	Drop group 4, side B reference fail	—	17
( )-LG1A*	NSA	MN/MN	Line group 1, side A reference fail	—	17
( )-LG1B*	NSA	MN/MN	Line group 1, side B reference fail	—	17
( )-LG2A*	NSA	MN/MN	Line group 2, side A reference fail	—	17
( )-LG2B*	NSA	MN/MN	Line group 2, side B reference fail	—	17
INHAUTOMODESW	NSA	MN/MN	Inhibit automatic restoration of primary timing reference	ABN (NEP)	53
LOCKOUTOFSYNC	NSA	MN/MN	Lock out of synchronization reference switching	—	—
OPRACT	NSA	MN/MN	Synchronization reference switch is in effect	ABN (NEP)	53
SYNCSWFAIL	NSA	MN/MN	Synchronization reference switch failure	—	—
MANSWTOPRI	—	Event	Manual switch to primary reference	—	—
MANSWTOSEC	—	Event	Manual switch to secondary reference	—	—
SWTOPRI	—	Event	Automatic switch to primary reference	—	—

Table AR. BITS Synchronization Sources

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
SWTOSEC	—	Event	Automatic switch to secondary reference	—	—
OPRSYNC-PRI	—	Condition	Operate synchronization on primary reference	—	—
OPRSYNC-SEC	—	Condition	Operate synchronization on secondary reference	—	—
* *( ) = PRI.*					

Table AS. CDAC Environmental Alarm Inputs

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
(ENV-1)	NSA	MN	User defined alarm 1	—	1
(ENV-2)	NSA	MN	User defined alarm 2	—	2
(ENV-3)	NSA	MN	User defined alarm 3	—	3
(ENV-4)	NSA	MN	User defined alarm 4	—	4
(ENV-5)	NSA	MN	User defined alarm 5	—	5
(ENV-6)	NSA	MN	User defined alarm 6	—	6
(ENV-7)	NSA	MN	User defined alarm 7	—	7
(ENV-8)	NSA	MN	User defined alarm 8	—	8
(ENV-9)	NSA	MN	User defined alarm 9	—	9
(ENV-10)	NSA	MN	User defined alarm 10	—	10
(ENV-11)	NSA	MN	User defined alarm 11	—	11
(ENV-12)	NSA	MN	User defined alarm 12	—	12

Table AT. Common Equipment/NE

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
ALMSYNC	NSA	MN	Alarms out of sync with COA LEDs	—	—
BAFFLEALM1	NSA	MJ	Baffle Alarm 1	—	14
BAFFLEALM2	NSA	MJ	Baffle Alarm 2	—	14
CONFIG	NSA	MN	Configuration error (upgrade)	ABN (NEP)	—
EQPTMA	NSA	MN	Equipment is OOS-MA-AS	—	—
FA	NSA	MN	Fuse alarm	—	13
FACMA	NSA	MN	A facility is OOS-MA-AS	—	—
FANALM	NSA	MN	Fan alarm detected	—	14
INVERR	NSA	MN	Shelf inventory (fuse checksum) error	—	—
LOGBUFR90-SECURITY	NSA	NA	Security log buffer is 90% full	—	—
LOGBUFR90-SYSTEM	NSA	NA	System message log buffer is 90% full	—	—
LOGBUFROVFL-SECURITY	NSA	NA	Security log buffer overflow	—	—
LOGBUFROVFL-SYSTEM	NSA	NA	System message log buffer overflow	—	—
MEA	NSA	MN	Shelf ID mismatch with NEP software version	—	—
PATHMA	NSA	MN	A cross-connected STS or VT1 path is OOS-MA-AS	—	—
PROGVER	NSA	MN	Program version error (no program on flash disk matches the NEP version)	ABN (NEP)	—
PWRF-48VA	NSA	MN	Power fail -48V A	—	—
PWRF-48VB	NSA	MN	Power fail -48V B	—	—
SECU-INTRU	NSA	MN	Security intrusion alert	—	—
SYNCMA	NSA	MN	A provisioned synchronization (NESYNC/BITSSYNC) is OOS-MA-AS	—	—
ALMLVL-CL	—	Event	Alarm level is clear	—	—
ALMLVL-CR	—	Event	Alarm level is critical	—	—
ALMLVL-MJ	—	Event	Alarm level is major	—	—
ALMLVL-MN	—	Event	Alarm level is minor	—	—
BUFROVLD	—	Event	Session overload	—	—

Table AT. Common Equipment/NE (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
CAMRBUFROVFL	—	Event	CAMR buffer overflow	—	—
OSDRPMSG	—	Event	OS gateway has dropped a message	—	—
PROCROVLD	—	Event	Processor overload	—	—
PROGCHK	—	Event	Flash disk corrupt (read access attempt fails)	—	—
RMTDL	—	Event	Remote download to flash disk in progress	—	—
RMTDLFAIL	—	Event	Remote download to flash disk failed	—	—
ACOACT	—	Condition	Alarm cut-off active	—	—
ACODELD	—	Condition	Alarm cut-off delayed	—	—
ACOIMED	—	Condition	Alarm cut-off immediate	—	—
ACOMAN	—	Condition	Alarm cut-off manual	—	—
ADM	—	Condition	NE type: Add/Drop Multiplexer	—	—
INHMSG	—	Condition	All autonomous messages inhibited	—	—
INHMSG-CR	—	Condition	Critical autonomous messages inhibited	—	—
INHMSG-MJ	—	Condition	Major autonomous messages inhibited	—	—
INHMSG-MN	—	Condition	Minor autonomous messages inhibited	—	—
INHMSG-NA	—	Condition	Not alarmed autonomous messages inhibited	—	—
LINEAR	—	Condition	NE supports line operation only	—	—
RING	—	Condition	NE supports line and ring operation	—	—
SWDL	—	Condition	Software download in progress – automatic or manual	—	—
TM	—	Condition	NE type: Terminal Multiplexer	—	—
UPSR–xxx where xxx = LG1, LG2, DG1, DG2, DG3, DG4, DG1A, DG2A, DG3A, DG4A, DG1B, DG2B, DG3B, or DG4B	—	Condition	Some UPSR paths are on LG1, LG2, DG1, DG2, DG3, DG4, DG1A, DG2A, DG3A, DG4A, DG1B, DG2B, DG3B, or DG4B	—	—

Table AT. Common Equipment/NE

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
VTGRP	—	Condition	VT1/T1 grouped numbering enabled	—	—
VTSEQ	—	Condition	VT1/T1 sequential numbering enabled	—	—

Table AU. Ports (Craft 1, Craft 2, SE2A, X.25, and PPP)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
CD	NSA	MN	Port failure	—	—
LINKSTATE	—	—	Indicates the PPP link status	—	—

Table AV. IP Tunnel

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
EOC	NSA	MN	Embedded operations channel failure	—	—

Table AW. LLSDCC/LLSMLDCC

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT [3]	DESCRIPTION	LED	SERIAL E2A BIT
EOC	NSA	MN	Embedded operations channel failure	—	—
[3] *The ACT setting is used as default for both A & B sides when parent equipment (OCn based LIF's only) is provisioned SIMPLEX.*					

Table AX. Local Area Network (LAN)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
CARLOS	NSA	MN	Loss-of-carrier	—	—
DUPADR	NSA	MN	Duplicate address error	—	—
EXCOL	—	Event	Excessive collisions	—	—

Table AY. NE Synchronization Sources

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
( )-DG1A-n* where: n = 1...4	NSA	MN/MN	Drop group 1, side A reference fail	—	17
( )-DG1B-n* where: n = 1...4	NSA	MN/MN	Drop group 1, side B reference fail	—	17
( )-DG2A-n* where: n = 1...4	NSA	MN/MN	Drop group 2, side A reference fail	—	17
( )-DG2B-n* where: n = 1...4	NSA	MN/MN	Drop group 2, side B reference fail	—	17
( )-DG3A-n* where: n = 1...4	NSA	MN/MN	Drop group 3, side A reference fail	—	17
( )-DG3B-n* where: n = 1...4	NSA	MN/MN	Drop group 3, side B reference fail	—	17
( )-DG4A-n* where: n = 1...4	NSA	MN/MN	Drop group 4, side A reference fail	—	17
( )-DG4B-n* where: n = 1...4	NSA	MN/MN	Drop group 4, side B reference fail	—	17
( )-LG1A*	NSA	MN/MN	Line group 1, side A reference fail	—	17
( )-LG1B*	NSA	MN/MN	Line group 1, side B reference fail	—	17
( )-LG2A*	NSA	MN/MN	Line group 2, side A reference fail	—	17
( )-LG2B*	NSA	MN/MN	Line group 2, side B reference fail	—	17
( )-SYNCPRI*	NSA	MN/MN	Sync primary BITS input reference fail	—	17
( )-SYNCSEC*	NSA	MN/MN	Sync secondary BITS input reference fail	—	17
FRNG	NSA	NA/NA	Free run synchronization mode	—	—

Table AY. NE Synchronization Sources (cont)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
FST	NSA	MN/MN	Fast synchronization mode	—	—
HLDOVR	NSA	MN/MN	Synchronization is in holdover mode	—	—
INHAUTOMODESW	NSA	MN/MN	Automatic switching to primary timing reference is inhibited	ABN (NEP)	53
INHPMREPT	NSA	NR/NR	All scheduled PM reports inhibited	—	—
OPRACT	NSA	MN/MN	Synchronization reference operate active	ABN (NEP)	53
LOCKOUTOFSYNC	NSA	MN/MN	Lock out of synchronization reference switching	—	—
SYNC	SA	MJ/MN	High speed synchronization failure	—	—
SYNCSWFAIL	NSA	MN/MN	Synchronization reference switch failure	—	—
MANSWTOPRI	—	Event	Manual switch to primary reference	—	—
MANSWTOSEC	—	Event	Manual switch to secondary reference	—	—
MANSWTOTHIRD	—	Event	Manual switch to third priority reference	—	—
MANSWTOFOURTH	—	Event	Manual switch to fourth priority reference	—	—
MANSWTOFIFTH	—	Event	Manual switch to fifth priority reference	—	—
SWTOPRI	—	Event	Automatic switch to primary reference	—	—
SWTOSEC	—	Event	Automatic switch to secondary reference	—	—
SWTOTHIRD	—	Event	Automatic switch to third priority reference	—	—
SWTOFOURTH	—	Event	Automatic switch to fourth priority reference	—	—
SWTOFIFTH	—	Event	Automatic switch to fifth priority reference	—	—
SWTOINT	—	Event	Automatic switch to internal clock reference	—	—
DELAYSWSYNC	—	Condition	Synchronization switch mode is delayed (provisioned)	—	—

Table AY. NE Synchronization Sources

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
FRNGSYNC	—	Condition	Free running synchronization mode (provisioned)	—	—
FSTSYNC	—	Condition	Fast start synchronization mode (provisioned)	—	—
HLDOVRSYNC	—	Condition	Hold-over synchronization mode (provisioned)	—	—
IMEDSWSYNC	—	Condition	Synchronization switch mode is immediate (provisioned)	—	—
OPRSYNC-PRI	—	Condition	Operate synchronization on primary reference	—	—
OPRSYNC-SEC	—	Condition	Operate synchronization on secondary reference	—	—
OPRSYNC-THIRD	—	Condition	Operate synchronization on third reference	—	—
OPRSYNC-FOURTH	—	Condition	Operate synchronization on fourth reference	—	—
OPRSYNC-FIFTH	—	Condition	Operate synchronization on fifth reference	—	—
* *( ) = PRI, SEC, THIRD, FOURTH or FIFTH.*					

Table AZ. Network

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
CDACCONN	NSA	MN	CDAC connection failure	—	—
CDACPROV	NSA	MN	CDAC misprovisioned	—	—
E2ACONN	NSA	MN	E2A gateway connection failure	—	—
RADCONN	NSA	MN	CAMR connection failure	—	—
RADPROV	NSA	MN	Far end alarm misprovisioned	—	—

Table BA. POS Port

ALARM CONDITION	SRVCE-AFFCTG	DEFAULT NTFCNCDE A/B	DESCRIPTION	LED	SERIAL E2A BIT
INVLDADRCTL	NSA	MN/MN	Invalid address control field	—	—
INHPMREPTQOS	NSA	NR/NR	Inhibit scheduled QOS PM reports	—	—
INHPMREPTNDC	NSA	NR/NR	Inhibit scheduled NDC PM reports	—	—
T-ABTPKT	NSA	NA/NA	Aborted packet TCA*	—	—
T-DISFR	NSA	NA/NA	Received frames discarded TCA*	—	—
T-FCSERR	NSA	NA/NA	Frame with bad FCS TCA*	—	—
T-LPKT	NSA	NA/NA	Packet longer than max length TCA*	—	—
T-SPKT	NSA	NA/NA	Packet shorter than min length TCA*	—	—
* *Either 15-minute or 1-day Threshold Crossing Alert (TCA).*					

Table BB. Remote NE

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
RMTALM	NSA	MN	Remote NE alarm indication	—	—

Table BC. Synchronous Maintenance Link (SML) Facility

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AIS	NSA	NR	Alarm indication signal detected	—	—
AISYEL	NSA	NR	AIS yellow detected	—	—
BER-HT	NSA	MN	Signal failure bit error rate threshold crossed	—	—
LOF	NSA	MN	Loss-of-frame	—	—
LOS	NSA	MN	Loss-of-signal	—	—
MTCE	NSA	MN	Removed from service for maintenance	ABN (NEP)	53
YEL	NSA	NR	Yellow (facility) detected	—	—

Table BD. Target Identifier Address Resolution Mapping (TADRMAP)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
TADRMM	NSA	MN	TADRMAP provisioning mismatch	—	—
TARPCACHEFLSHD	—	Event	TARP cache has been flushed	—	—

Table BE. USRLAN: LIF901

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
INHPMREPTQOS	NSA	NR/NR	QOS PM report inhibited	—	—
INHPMREPTNDC	NSA	NR/NR	NDC PM report inhibited	—	—
LOS	SA	CR/CR	Loss-of-signal	SFn where n = 1...4	30, 33
MTCE	NSA	MN/MN	Remove from service for maintenance	ABN (NEP)	53
T-CSERR	NSA	NA/NA	Number of RCV carrier sense errors TCA*	—	—
T-DISFR	NSA	NA/NA	RCV frames discarded due to no buffer available TCA*	—	—
T-EXCOL	NSA	NA/NA	Number of TRMT excessive collisions TCA*	—	—
T-FRCRC	NSA	NA/NA	Number of RCV frames with bad FCS TCA*	—	—
T-LFR	NSA	NA/NA	Number of RCV frames longer than maximum TCA*	—	—
T-LFRCOL	NSA	NA/NA	TRMT late transmit collisions TCA*	—	—
AINS	—	Event/ Condition	Automatic In-Service state	—	—
IS-AUTO	—	Event	Automatic OOS-MA to in-service	—	—

* *Either 15-minutes or 1-day Threshold Crossing Alert (TCA).*

Table BF. USRLAN: LIFG01

ALARM CONDITION	SRVCE-AFFCTG	DEFAULT NTFCNCDE A/B	DESCRIPTION	LED	SERIAL E2A BIT
INHPMREPTQOS	NSA	NR/NR	QOS PM report inhibited	—	—
INHPMREPTNDC	NSA	NR/NR	NDC PM report inhibited	—	—
LINENA	SA	CR/CR	Line not available	SF	30, 33
LOS	SA	CR/CR	Loss-of-signal	SF	30, 33
LPR	NSA	MN/MN	Low laser light	—	—
MTCE	NSA	MN/MN	Removed from service for maintenance	ABN (NEP)	53
T-DISFR	NSA	NA/NA	Number of RCV frames discarded due to no buffer available TCA*	—	—
T-EXCOL	NSA	NA/NA	Number of TRMT excessive collisions TCA*	—	—
T-FRCRC	NSA	NA/NA	Number of RCV frames with bad FCS TCA*	—	—
T-LFR	NSA	NA/NA	Number of RCV frames longer than maximum TCA*	—	—
T-LFRCOL	NSA	NA/NA	Number of TRMT late transmit collisions TCA*	—	—
T-SFR	NSA	NA/NA	Number of RCV frames shorter than minimum TCA*	—	—
AINS	—	Event/ Condition	Automatic In-Service state	—	—
IS-AUTO	—	Event	Automatic OOS-MA to in-service	—	—

* *Either 15-minutes or 1-day Threshold Crossing Alert (TCA).*

Table BG. Virtual Channel (VCL)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AIS	SA	NR	Alarm indication signal	—	—
RFI	SA	NR	VC Remote Defect Indicator	—	—
LOSSCONTSE	SA	MN	Loss of VC segment continuity	—	—
LOSSCONTCE	SA	MN	Loss of VC connection continuity	—	—
INHCONTSE	NSA	NR	Remote activation of VC segment continuity inhibited	—	—
INHCONTCE	NSA	NR	Remote activation of VC connection continuity inhibited	—	—
INHPMSE	NSA	NR	Remote activation of VC segment PM inhibited	—	—
INHPMCE	NSA	NR	Remote activation of VC connection PM inhibited	—	—
INHPMREPTSQOS	NSA	NR	Scheduled VC segment QOS PM reports inhibited	—	—
INHPMREPTCQOS	NSA	NR	Scheduled VC connection QOS PM reports inhibited	—	—
T-LOS0+1	NSA	NA	RX total lost CLP0+1 cells TCA – NE or FE*	—	—
T-LOS0	NSA	NA	RX total lost CLP0 cells TCA – NE or FE*	—	—
T-SECB	NSA	NA	RX severely errored cell block TCA – NE or FE*	—	—
T-IMP0+1	NSA	NA	RX impaired cell block TCA – NE or FE*	—	—
ACTCONTSE	—	Event/ Condition	VC segment continuity cells sourced – NE or FE	—	—
ACTCONTCE	—	Event/ Condition	VC connection coninuity cells sourced – NE or FE	—	—
ACTFWDMONSE	—	Event/ Condition	VC segment PM forward monitoring cells sourced – NE or FE	—	—
ACTFWDMONCE	—	Event/ Condition	VC connection PM forward monitoring cells sourced – NE or FE	—	—
ACTBKWDRPTSE	—	Event/ Condition	VC segment PM backward report cells sourced – NE or FE	—	—
ACTBKWDRPTCE	—	Event/ Condition	VC connection PM backward report cells sourced – NE or FE	—	—

Table BG. Virtual Channel (VCL)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AISLOC	—	Condition	VC automatic in-service defect location displayed as comment	—	—
RDILOC	—	Condition	VC RDI defect location displayed as comment	—	—
* *Either 15-minutes or 1-day Threshold Crossing Alert (TCA).*					

Table BH. Virtual Path (VPL)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
AIS	SA	NR	Alarm indication signal	—	—
RFI	SA	NR	VP Remote Defect Indicator	—	—
LOSSCONTSE	SA	MN	Loss of VP segment continuity	—	—
LOSSCONTCE	SA	MN	Loss of VP connection continuity	—	—
INHCONTSE	NSA	NR	Remote activation of VP segment continuity inhibited	—	—
INHCONTCE	NSA	NR	Remote activation of VP connection continuity inhibited	—	—
INHPMSE	NSA	NR	Remote activation of VP segment PM inhibited	—	—
INHPMCE	NSA	NR	Remote activation of VP connection PM inhibited	—	—
INHPMREPTSQOS	NSA	NR	Scheduled VP segment QOS PM reports inhibited	—	—
INHPMREPTCQOS	NSA	NR	Scheduled VP connection QOS PM reports inhibited	—	—
T-LOS0+1	NSA	NA	RX total lost CLP0+1 cells TCA* – NE or FE	—	—
T-LOS0	NSA	NA	RX total lost CLP0 cells TCA* – NE or FE	—	—
T-SECB	NSA	NA	RX severely errored cell block TCA* – NE or FE	—	—
T-IMP0+1	NSA	NA	RX impaired cell block TCA* – NE or FE	—	—
ACTCONTSE	—	Event/ Condition	VP segment continuity cells being transmitted (NE) or received (FE)	—	—

Table BH. Virtual Path (VPL)

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
ACTCONTCE	—	Event/ Condition	VP connection continuity cells being transmitted (NE) or received (FE)	—	—
ACTFWDMONSE	—	Event/ Condition	VP segment forward monitoring PM cells being transmitted (NE) or received (FE)	—	—
ACTFWDMONCE	—	Event/ Condition	VP connection forward monitoring PM cells being transmitted (NE) or received (FE)	—	—
ACTBKWDRPTSE	—	Event/ Condition	VP segment backward reporting PM cells being transmitted (NE) or received (FE)	—	—
ACTBKWDRPTCE	—	Event/ Condition	VP connection backward reporting PM cells being transmitted (NE) or received (FE)	—	—
AISLOC	—	Condition	VP automatic in-service defect location displayed as comment	—	—
RDILOC	—	Condition	VP RDI defect location displayed as comment	—	—

* *Either 15-minutes or 1-day Threshold Crossing Alert (TCA).*

Table BI. X.25 Protocol Stack

ALARM CONDITION	SRVCE-AFFCTG (ACTIVE)	DEFAULT NTFCNCDE ACT/STBY	DESCRIPTION	LED	SERIAL E2A BIT
LAPBERR	NSA	MN	Link Access Protocol B link failure	—	—

TNG-512
System Management Philosophy

1. Introduction

1.1 For a Network Element (NE) to provide its users with efficient and economical service, the NE must be managed properly. Management of 1603 SMX NE entails two primary responsibilities:

- Monitoring performance to make decisions that relate to optimizing performance and system efficiency.
- Performing tasks that relate to the overall management and control of the system.

1.2 This document provides general information about the system management considerations and tasks related to the 1603 SMX NE.

2. Operational Tasks

2.1 The 1603 SMX typically runs with minimal operator intervention. However, operator (craft) interaction is required for the following tasks:

- To install and turn up the system.
- To determine security functions for users, commands, and access channels (OS and ports).
- To isolate troubles and replace defective units.
- To add service not originally provisioned on the initial turn-up.

3. Security

3.1 NE security refers to the measures taken to prevent unauthorized personnel from browsing, altering or destroying NE specific information/provisioning and system performance monitoring/alarm data. In so doing, the integrity of the network also is protected.

3.2 Achieving and maintaining confidence in a security system is dependent on certain environmental factors, such as personnel and the facilities. Companies must ensure that users honor system controls, and that a reasonable amount of physical security measures exist to prevent sabotage and vandalism. In addition, privileges must be assigned with discretion.

4. Privileges

4.1 System management functions require privileges. Assigning privileges restricts certain users from performing certain system activities. These restrictions protect the integrity of the operating system's performance and the integrity of service provided to customers.

4.2 Privileges should be granted to users on the basis of two factors: (1) does the user have a legitimate need for the privilege, and (2) does the user have the skill and expertise required to avoid service disruption. Never issue "all" privileges to all users. Such indiscriminate assignment will invite user probing, user penetration (breaking controls), and other service-affecting tampering. Refer to TNG-510 for details on system security.

5. Performance Monitoring

5.1 Performance monitoring has two purposes: (1) to identify network problems that need to be addressed to optimize performance, and (2) to recognize NE specific hardware problems that impact performance. System tuning and workload management are time-consuming activities that require both familiarity with the systems (hardware and software that make up the NEs) and the network's design.

5.2 System performance (i.e., bit error rate, slip counts, bipolar violations, etc.) is monitored in real time and reported periodically (on a selectable time interval basis) or on demand. Alarm reporting thresholds are also selectable.

5.3 Hardware problems are a common source of performance complaints. When NEs go off-line or an NE goes into a degraded state, the network performance is affected. Timely identification of the source of the problem will expedite performance recovery. Fault location consists of detecting a fault, verifying the fault, attempting automatic recovery or protection, and trouble notification.

6. Remote Inventory Interrogation

6.1 From time to time, the OS may need to determine exactly what the plug-in configurations are for specific NEs, as well as the current system software version. The 1603 SMX provides remote inventory and software version interrogation through the remote craft port on the COA plug-in.

TNG-514
Network Element Service States

1. General

1.1 This document provides a description of the management states of equipment or facilities associated with Alcatel's SONET Network Element (NE). The management states used in the 1603 SMX are based on a subset of the specifications in Bellcore Technical Advisory TA-NWT-001093 Issue 1, October 1990 (Generic State Model for Managing Network Elements). Only the specifications applicable to Alcatel's NEs are described here.

1.2 The management state of an object (equipment or facility) represents its current condition of availability and operability, or its service ability. A variety of state attributes is available that expresses and controls aspects of the operation of the object. The purpose of having management states is to control the general availability, and, if an object cannot provide service, to indicate the action to take to restore service.

1.3 When the state of an object is retrieved, the response provides the current status of an object's availability to perform its service function as defined by the object attributes. And, if possible, supplemental information is provided about associated objects that support the object or that are supported by the object. Certain TL1 commands have additional parameters that allow the states of an object to be entered or modified.

1.4 The state of an object is represented by three parameters: the Primary State (PST), the Secondary State (SST), and the Associated State (AST).

2. Primary State

2.1 The Primary State (PST) indicates the service availability of an object and consists of two components: Service Condition and Service Condition Qualifier. The Service Condition component is required for PST while the Service Condition Qualifier is optional.

- **Service Condition:** The Service Condition component is applicable to most object types and places the object in one of two possible states:
  - **In-Service (IS):** The object is performing or is available to perform all or part of its designed service functions; or
  - **Out-Of-Service (OOS):** In general, the object is not available to perform any of its designed service functions.

- **Service Condition Qualifier:** When the service condition is IS, the qualifier indicates whether the object is able to perform all or only part of its designed service functions. If an object is able to perform all of its designed service functions, it is considered to be Normal (NR); otherwise, it is Abnormal (ANR). Whether an NE is NR or ANR is automatically updated by the NE according to the current service condition of the object. The OS or craft has no control over the qualifier for IS.

2.2 When the service condition is OOS, the qualifier indicates which operations domain is responsible for causing the OOS condition or for putting the object back to IS. For Alcatel SONET NEs, there are two applicable operation domains: provisioning driven Memory Administration (MA) and Maintenance (MT). The distinctions between these two qualifiers are:

- MA deals with the provisioning process, primary resource/service parameter assignment (e.g., database parameters), and equipage (e.g., detecting the presence or absence of plug-ins).

- MT deals with the fault detection and service recovery. MT also deals with testing that is done to ensure an object is functioning properly or to sectionalize and isolate a suspected or known trouble condition. Faults may be detected automatically (e.g., because of poor performance and exceeding a threshold level) or by testing (initiated automatically by the object itself or by a testing craftsperson/OS). Depending on the severity of the trouble, the object may be left IS and marked abnormal (ANR) or taken OOS for a specific cause that is indicated by the supplemental information.

2.3 The PST parameter can be present in the input and normal response to a command that uses the Retrieve (RTRV) verb. Possible output values for the retrieve command are listed in Table A.

Table A. Output Values

VALUE	DESCRIPTION
IS-NR	Object is in-service and normal
IS-ANR	Object is in-service but an abnormal condition exists. It may be able to perform all or only part of its designed service function (e.g., due to degrade)
OOS-MA-AS	Out-of-service state for provisioning activity; object has been assigned
OOS-MA-UAS	Out-of-service state for provisioning activity; object has not been assigned
OOS-MT	Out-of-service state for maintenance activity such as fault, performance monitoring, or testing; object has been assigned

2.4 When PST (Primary State) is used in commands that use Enter (ENT) or Edit (ED) verbs, the value indicates the desired Primary State of the object. When used in the Enter command, if PST is not specified, it defaults to IS. When used in the Edit commands, if PST is not specified, the current value of PST does not change. Only certain input values may be specified for PST using the Enter or Edit commands. Valid input values are listed in Table B.

Table B. Input Values

VALUE	DESCRIPTION
IS	In-Service; IS [-(NR or ANR)] implied; whether NR (normal) or ANR (abnormal) is determined by the NE
OOS	Out-Of-Service; OOS-MA implied
MA	Memory Administration; OOS-MA implied (synonymous with OOS)
MT	Maintenance; OOS-MT implied

2.5 An example command entry for changing the primary BITS facility to the OOS-MA state is:

ED-BITS::SYNCPRI:::::OOS;

2.6 There are other TL1 verbs available for manipulating the state of an object. They are listed in Table C.

Table C. TL1 Verbs

VALUE	DESCRIPTION
DLT	DELETE (e.g., DLT-BITS). This verb is used in a command to delete the provisioning information concerning an object from the NE database. It effectively sets the object's PST parameter to OOS-MA-UAS
RMV	REMOVE (e.g., RMV-BITS). This verb is used in a command to place the object in the maintenance state (PST = OOS-MT). The object is able to carry traffic but alarm detection and reporting are suspended
RST	RESTORE (e.g., RST-BITS). This verb is used in a command to restore the object from the maintenance state to its previous state, if possible

2.7 Certain guidelines and restrictions that apply when manipulating the state of an object are summarized as follows:

- The ENT (Enter) command is only valid if the object is unassigned (PST = OOS-MA-UAS). This verb is used in a command to add a new object to the current configuration.

- To Edit parameters other than (controllable) PST and/or SST parameters, the primary state of the object must be OOS-MA-AS. The Edit command is also used to change the primary state of the object. This ability is useful, for example, to change the primary state of the object to OOS-MA-AS. This allows editing of the other parameters (other than PST and/or SST) and then returns the object to its previous state (e.g., from IS to OOS-MA-AS and back).

- To Delete the object, the primary state must not be unassigned (PST ≠ OOS-MA-UAS). The DELETE function removes the object from the current configuration.

- The Remove (RMV) command is used to place an object in the maintenance state for testing. It is only valid if the primary state is In-Service (PST = IS-NR or IS-ANR). Otherwise, the edit command must be used (i.e., from OOS-MA to OOS-MT).

- The Restore (RST) command is used to return an object from the maintenance state (OOS-MT) to the In-Service state (IS). It is only valid when PST = OOS-MT.

2.8 The execution of a command may be denied if a possible service interruption is detected or if the object is in an incorrect state.

3. Secondary State

3.1 The Secondary State (SST) provides supplementary information on the state of an object. Such information may consist of detailed reasons for being in a particular primary state, or supplemental information useful in managing the object.

3.2 Values of SST are specific to the objects and PST. Not all values of SST are applicable to all objects or all values of PST. Some values of SST may apply only if the object is equipment or a facility. Depending on the current state, an object may possess zero or many values of the SST.

3.3 Some values of the SST can only be changed by the NE itself to reflect the current status of the object. These values are read-only (e.g., from the NORMAL RESPONSE of the Retrieve command). Some SST parameters are also controllable by an OS or craftperson to impose control on the object.

3.4 When a value of SST is used in the input of commands with the Enter (ENT) or Edit (ED) verbs, this value specifies the desired secondary state, (i.e., the state to be activated or staying active if it has already been activated). Table D lists the only controllable value for SST parameter.

Table D. Controllable Value for SST Parameter

VALUE	DESCRIPTION
AINS	Automatic In-Service; the equipment is automatically placed In-Service (PST = IS) when installed or plugged in. This value, when used as an input, allows pre-provisioning of uninstalled equipment using the Enter command, effectively placing the equipment in the OOS-MA-AS, unequipped state.
AINS-DEA	Automatic-In-Service Deactivate. Turns off the automatic in-service state.

3.5 When a value of SST appears in the normal response of the Retrieve command, it indicates that the value is currently active. Table E lists valid output values.

Table E. Output Values

VALUE	DESCRIPTION
ACT	Active; this equipment is currently providing service (versus standby)
AINS	Automatic In-service; the equipment is automatically placed In-Service (pst = IS) when plugged in
APSI	Automatic Protection Switch Inhibited; for a protected entity, it is equivalent to lock-on. For a protecting entity, it is equivalent to lock-out
BOOT	Processor is running bootcode (requires download or CPY-MEM)
DX	Configuration is duplex
EQ	Equipped; the entity has been equipped with the necessary equipment (plugged in)
FLT	Fault; the equipment is OOS-MT because it is faulty
FRCD	Forced; change of state was forced
MAN	Manual; the equipment has been manually taken OOS-MT for maintenance activities
MEA	Mismatch of equipment and attributes; the equipped object does not match the provisioned object
OVFL	Overflow; for the LOG and Database Capture Buffer (DBCB) objects that are not provisioned with wrap buffer, this indicates that the object has depleted its memory resources, i.e., no additional storage (memory) to capture more records
PROT	Entity is Protection (not working) side
PWR	Power; entity is OOS-MT because it has no power
STBY	Standby; this entity is not currently providing service
SWDL	Software downloaded
SWVERR	Software version error
SX	Configuration is simplex

Table E. Output Values (cont)

VALUE	DESCRIPTION
TB	Diagnostic test busy
TSTF	Test failure; the equipment is OOS-MT because of test failure
UEQ	Unequipped; the entity is not equipped with the necessary equipment
WORK	Entity is working side

4. Associated State

4.1 The Associated State (AST) parameter provides additional information regarding the existence and service availability of the associated objects for the specified object. The associated objects fall into two categories: Supporting Object and Supported Object. Objects that require support from other objects in order to provide services are called Supported Objects, and the objects that provide support are called Supporting Objects. A supporting object may provide support by controlling or containing the supported object. For example, a high speed OC3, OC12, or OC48 facility's ability to provide normal service may depend on the service state of its associated HIF plug-in unit. Therefore, the OC3, OC12, or OC48 facility is the Supported Object, and the HIF plug-in is the Supporting Object. Before the OC3, OC12, or OC48 facility can be provisioned in service, the supporting HIF plug-in must be placed in service. Likewise, before the HIF plug-in can be deleted, the supported OC3, OC12, or OC48 facility must first be deleted.

4.2 When a value of AST appears in the normal response of a Retrieve command, it indicates that the value is currently active. Table F lists valid output values.

Table F. Output Values

VALUE	DESCRIPTION
FAF	Facility Failure; associated supporting facility is OOS
FEF	Family of Equipment Failure; associated controlling equipment is OOS
SEA	Supported Entity Assigned; one or more entities that this equipment directly supports are assigned (FUTURE)
SEO	Supported Entity Outage (FUTURE)
UEA	Underlying Entity Abnormal; the associated supporting entity is IS-ANR or OOS

5. State Transition Diagrams

5.1 A graphical representation showing the effects on the service states of an object as a result of various input commands and events can be useful in understanding the concepts required to effectively turn up and maintain an NE. A state transition diagram is typically used to show the interrelationship between input commands/events and the NE service states.

5.2 Figure 1 shows a state transition diagram of the facilities associated with the 1603 SMX. Figure 2 shows a state transition diagram for the 1603 SMX equipment (plug-in units). The boxes in Figures 1 and 2 represent the states. Each line between the boxes represents the input command verb or event that causes a transition from one state to another. Each box contains a primary state and may contain one or more secondary states. The secondary states are listed below the primary state. Not all states are shown. Only the states that are affected by input commands that directly alter the primary state and the controllable secondary state [AINS[for equipment are shown. Input events shown in both tables are degradation, failures, recovery from a degradation or failure. For equipment, the effects of the insertion and removal of plug-ins are also shown.

5.3 When the 1603 SMX system is first equipped and turned up, the equipment and facilities are in predetermined default states. Most equipment and facilities are in the OOS-MA-UAS state and must be entered into service. However, some equipment, such as the COA and NEP plug-ins, are required to come-up in-service to allow processing and communications with the NE.

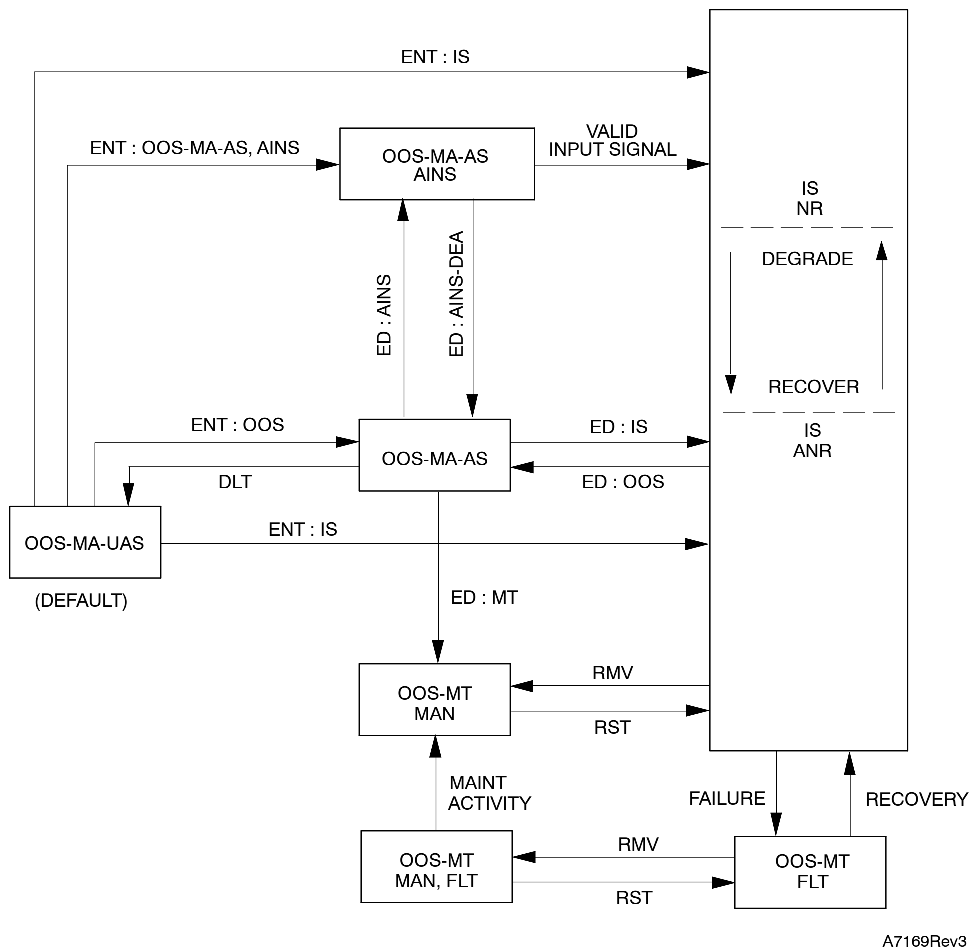


Figure 1. State Transition Diagram for Facilities Associated with the 1603 SMX

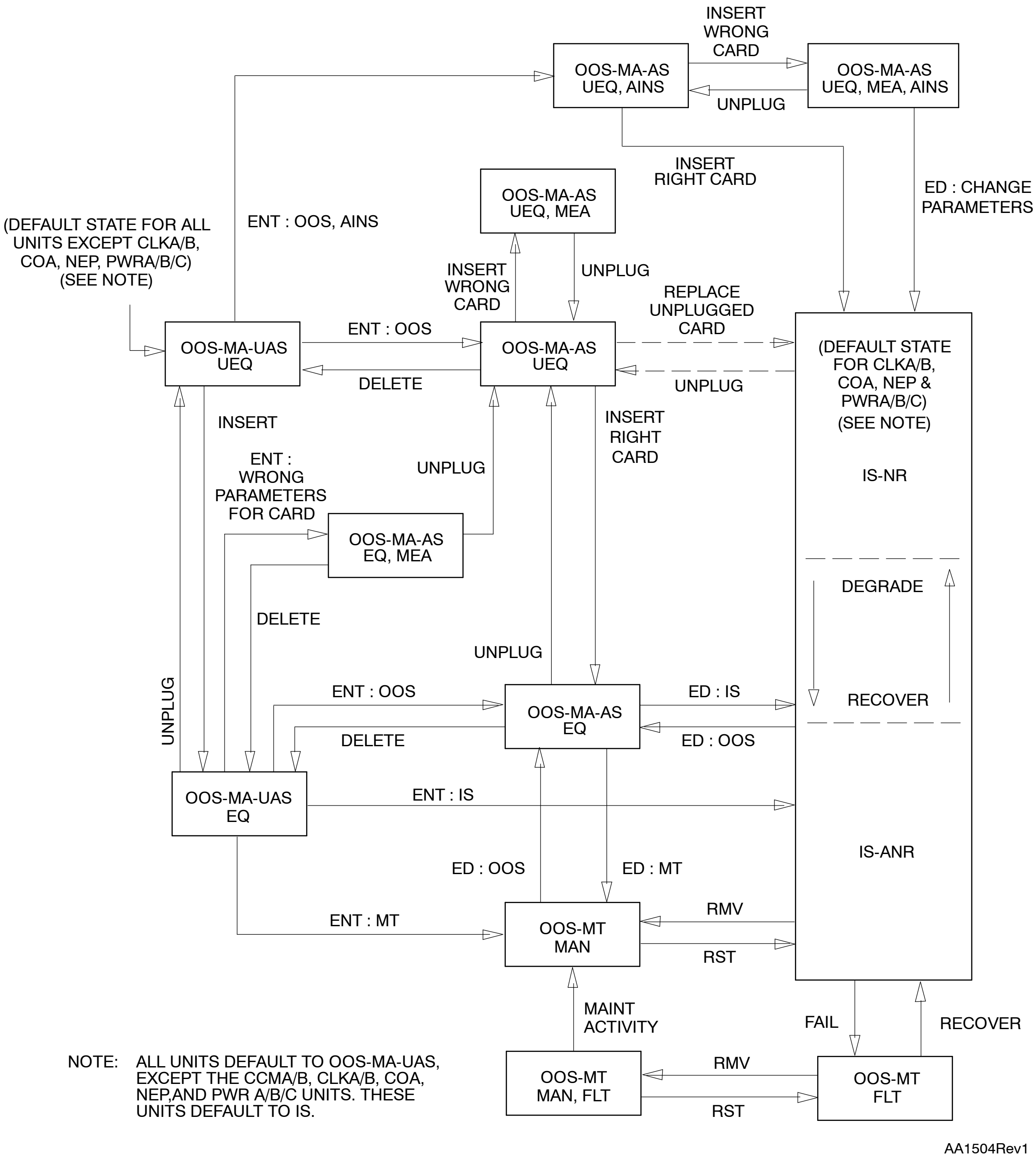


Figure 2. State Transition Diagram for 1603 SMX Equipment