



***WaveStar*[™] DACS 4/4/1, releases 3.0 and 3.1**

Maintenance guide



This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts or licensing, without the express written consent of Lucent Technologies and the business management owner of the material.

Product Development Manager 1 800 645 6759 (continental U.S.)
1 317 322 6847

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

CE Notice

Trademarks

Windows NT is a registered trademark of Microsoft Corporation.

Support

If you need technical assistance, contact your local field support organisation. They will either resolve your request or escalate it as necessary.

For comments or questions about this document, or to report an error, call +1 317-322-6847.

Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations



WaveStar™ DACS 4/4/1, releases 3.0 and 3.1
Maintenance guide

365-367-513 Issue 3 July 2002

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

1. Was the information product:

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

Please provide any additional comments:

2. Please rate the effectiveness of this information product:

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

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

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

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

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

Name: _____ Date: _____

Company/organization: _____ Telephone number: _____

Address: _____

Email address: _____ Job function: _____

If you choose to complete this form online, go to <http://www.lucent-info.com/comments>

Otherwise fax to 407 767 2760 (U.S.) or +1 407 767 2760 (outside the U.S.) or email comments to ctiphotline@lucent.com



Lucent Technologies values your comments!

Lucent Technologies
Bell Labs Innovations



WaveStar™ DACS 4/4/1, releases 3.0 and 3.1
Maintenance guide

365-367-513 Issue 3 July 2002

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

1. Was the information product:

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

Please provide any additional comments:

2. Please rate the effectiveness of this information product:

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

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

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

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

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

Name: _____ Date: _____

Company/organization: _____ Telephone number: _____

Address: _____

Email address: _____ Job function: _____

If you choose to complete this form online, go to <http://www.lucent-info.com/comments>

Otherwise fax to 407 767 2760 (U.S.) or +1 407 767 2760 (outside the U.S.) or email comments to ctiphotline@lucent.com





Contents

About this information product

Purpose	xxxiii
Reason for reissue	xxxiii
Safety labels	xxxiii
Intended audience	xxxiv
Conventions used	xxxiv
Related documentation	xxxiv
Related training	xxxv
How to order	xxxv

1 Product description

Overview	1-1
System description	
Overview	1-2
System description	1-3
System capacity	1-5
Control system	1-6
System interfaces	1-8
Synchronisation and timing	1-9

Equipment description

Overview	1-10
Equipment terms	1-11
Matrix and Synchronisation rack	1-12
Matrix and Synchronisation subrack	1-13
Bit Slice Switch Unit (BSSU)	1-15
Matrix and Control rack	1-16
Main Controller subrack	1-17
User Panel	1-20
Alarm Connector Panel (ACP)	1-22
Fan Connector Panel (FCP)	1-25
Bit Slice Switch Unit (BSSU)	1-26
Port rack	1-27
Port Subrack A (PSA)	1-28
Port Subrack C (PSC)	1-30
Port rack fan tray connector panel	1-32

2 About units and disks

Overview	2-1

Background information

Overview	2-2
Unit terms	2-3
About Electrostatic Discharge	2-4
Unit precautions	2-5

MO disks

Overview	2-6
About MO disks	2-7

Inserting an MO disk	2-8
Removing an MO disk	2-9
Units in the MS or port subrack	
Overview	2-10
Removing a unit from the MS or port subrack	2-11
Inserting a unit into the MS or port subrack	2-13
ARUs, LHUs, and PSPs	
Overview	2-15
About the ARU	2-16
About the LHU	2-18
About the PSP	2-19
MPUs and MSUs	
Overview	2-20
About the MPU	2-21
About the MSU	2-23
Serial TM, NIC TM, and SCSI TM	
Overview	2-24
About the NIC TM	2-25
About the SCSI TM	2-27
About the Serial TM	2-28
Unit codes and spare equipment list	
Overview	2-30
Unit codes	2-31
Recommended spare equipment	2-32

3 About cables

Overview	3-1

About cables	3-2
Inserting a cable	3-3
Removing a cable	3-4
About internal fibre connections	3-5

4 About the user interface

Overview	4-1
About the user-interface PC	4-2
Logging on	4-4
Logging off	4-6
Displaying the name of the system that the PC is connected to	4-7
Structure of the user interface	4-8
About the main application window	4-10
About query results windows	4-14
Updating data from a query results window	4-16
Button descriptions	4-17
Key descriptions	4-20
About system messages	4-22
About Help	4-23

5 About equipment and signal addresses

Overview	5-1
About entity addresses	5-2
About physical layer addresses	5-3
About signal layer addresses	5-4
Wildcard addresses	5-9
256 and 512 addressing	5-10
MC entity addresses	5-11

MS entity addresses	5-12
PSA entity addresses	5-13
PSC entity addresses	5-14
Equipment protection group addresses	5-16
MSP addresses	5-17
RT addresses	5-18
Fibre addresses	5-19

6 About alarms

Overview	6-1
Alarm terms	6-2
Defects and failures	6-3
Delay timers	6-4
Alarm Panel	6-5
User Panel	6-6
Conditions that affect service	6-7
Alarm indicator definition	6-8
Alarm indicator descriptions	6-9
MDIs and MDOs	6-10
About disconnecting and suppressing alarm indicators	6-12
About provisioning alarm indicators	6-13

7 Alarms

Overview	7-1
View Current Alarms window and procedures	
Overview	7-2
View Current Alarms window description	7-3
Querying all currently active alarms	7-4

View Current Alarms query results	7-5
Querying selected alarms	7-7
Station Alarm Control window and procedures	
Overview	7-8
Station Alarm Control window description	7-9
Querying the current state of the station alarms	7-10
Disconnecting, connecting, or suppressing station alarms	7-11
Display Alarm Panel and procedure	
Overview	7-12
Displaying the Alarm Panel	7-13

8 Reports

Overview	8-1
Background information	
Overview	8-2
About reports	8-3
Saving a report	8-5
Printing a report	8-6
Finding specific information in a report	8-7
Autonomous Messages window and procedures	
Overview	8-8
Autonomous Messages window description	8-9
Querying the last autonomous message	8-12
Querying all autonomous messages	8-13
Querying autonomous messages by specifying a time	8-14
Querying autonomous messages by specifying a message type or entity	8-15
Autonomous Messages query results	8-16

ALL query results	8-17
Alarms query results	8-18
Diagnostic Tests Completion Messages query results	8-19
Protection Switch Events query results	8-20
System Clock Reference Changes query results	8-21
Threshold Crossing Alerts query results	8-22
Unit State Changes query results	8-23
Port State Changes query results	8-24
Performance Monitoring window and procedures	
Overview	8-25
Performance Monitoring window description	8-26
Querying PM data	8-29
Performance Monitoring query results	8-30
User Transactions window and procedures	
Overview	8-34
User Transactions window description	8-35
Querying user transactions	8-37
User Transactions query results	8-38
Defects window and procedures	
Overview	8-39
Defects window description	8-40
Querying defects	8-42
Defects query results	8-43

9 Equipment protection switching

Overview	9-1

Background information

Overview	9-2
Which window to use	9-3
Equipment protection switching terms	9-4
Protection switching concepts	9-5
Protection switching priorities	9-7

MS Control window and procedures

Overview	9-8
MS Control window description	9-9
Querying the current status of MS Control	9-11
MS Control query results	9-12
MS Control Current Req descriptions	9-14
MS Control Current Req list of priorities	9-16
MS Control unit condition descriptions	9-17
Requesting an MS Control protection switch	9-18

Matrix Slice window and procedures

Overview	9-19
Matrix Slice window description	9-20
Querying the matrix slice	9-22
Matrix slice query results	9-23
Matrix slice Current Req descriptions	9-25
Matrix slice Current Req list of priorities	9-27
Matrix slice unit condition descriptions	9-28
Freezing the matrix slice	9-29
Clearing a freeze of the matrix slice	9-30
Forcing a switch to protection	9-31
Clearing a forced switch	9-32

Manually switching to protection	9-33
Clearing a manual switch	9-34
Locking service off of protection	9-35
Clearing a lock off	9-36
Locking service on to working	9-37
Clearing a lock on	9-38
DTU window and procedures	
Overview	9-39
DTU window description	9-40
Querying a DTU protection group	9-42
DTU query results	9-43
DTU Current Req descriptions	9-45
DTU Current Req list of priorities	9-47
DTU unit condition descriptions	9-48
Requesting a DTU protection group switch	9-49
STM1 1:8 window and procedures	
Overview	9-50
STM1 1:8 window description	9-51
Querying STM-1 1:8 protection groups	9-53
STM1 1:8 query results	9-54
STM1 1:8 Current Req descriptions	9-56
STM1 1:8 Current Req list of priorities	9-58
STM1 1:8 unit condition descriptions	9-59
Requesting an STM-1 1:8 protection switch	9-60
MC Control window and procedures	
Overview	9-61
MC Control window description	9-62

Querying the MC from the user interface	9-63
MC Control query results	9-64
Console screen procedures	
Overview	9-65
MC duplication terms	9-66
Console terminal connections	9-67
Getting to the MC Duplication Functions screen	9-68
Querying the MC from the console terminal	9-70
Requesting an MC protection switch	9-71

10 MSP and SNCP switching

Overview	10-1
Background information	
Overview	10-2
Switch request terms	10-3
MSP K byte mismatch state designations	10-5
ITU and ANSI MSP current requests, priorities, and unit conditions	
Overview	10-6
ITU and ANSI MSP Current Req values	10-7
ITU and ANSI MSP Current Req priorities	10-10
ITU and ANSI MSP unit condition values	10-11
NTT MSP current requests, priorities, and unit conditions	
Overview	10-12
NTT MSP Current Req values	10-13
NTT MSP Current Req priorities	10-21
NTT MSP unit condition values	10-23

MSP transmission window and procedures

Overview	10-24
MSP transmission window description	10-25
Querying MSP groups	10-28
MSP transmission query results	10-29
Requesting an MSP switch	10-31

SNCP current requests, priorities, and unit conditions

Overview	10-32
SNCP Current Request values	10-33
SNCP Current Request priorities	10-34
SNCP unit condition values	10-35

SNCP transmission window and procedures

Overview	10-36
SNCP transmission window description	10-37
Querying SNCP transmission groups	10-39
SNCP transmission query results	10-40
Requesting an SNCP switch	10-42

11 Controller maintenance

Overview	11-1

Background information

Overview	11-2
Controller maintenance tasks	11-3
Controller maintenance terms	11-4
Differences between cold and warm starts	11-5
About the MPU out-of-service state	11-6
About the SRC out-of-service state	11-7

Master and slave units	11-8
SRC states	11-9
Unit states	11-11
Unit ID values	11-13
Subrack Control window and procedures	
Overview	11-14
Subrack Control window description	11-15
Querying controllers	11-16
Subrack Control query results	11-17
Removing the MPU on a duplicated MC configuration	11-18
Removing the MPU on a single MC configuration	11-22
Restoring the DB on an MPU with a duplicated MC configuration	11-23
Restoring the DB on an MPU with a single MC configuration	11-29
Removing an MS subrack SRC from service	11-33
Removing a port subrack SRC from service	11-34
Restoring an SRC to service	11-35
Recovering from a Wrong unit in slot state	11-36
Unit Control window and procedures	
Overview	11-37
Unit Control window description	11-38
Initialising an SRC	11-40
Performing a warm start	11-41
Performing a cold start	11-42
Performing a cold start when the corresponding mate has a failure	11-44

12 Execute equipment tests

Overview	12-1

Background information

Overview	12-2
About the tests	12-3
Equipment diagnostic test terms	12-6
Foreground and background modes	12-8
Where to query diagnostic test results	12-9
Where the system displays diagnostic test results	12-10
Alarms and LEDs caused by diagnostic tests	12-11
Protection switching and diagnostic tests	12-12
Special equipment for diagnostic tests	12-13
About running diagnostic tests on more than one subrack	12-14
About removing units	12-15
About testing cables	12-16

Diagnostic Tests window

Overview	12-17
Diagnostic Tests window description	12-18

BCLAN diagnostic tests

Overview	12-20
BCLAN procedure	12-21
How to interpret BCLAN failure results	12-23
What to do if the BCLAN diagnostic test fails	12-26

DFWT diagnostic tests

Overview	12-27
How to install an attenuator	12-28
DFWT procedure for optical STM-1s	12-29
DFWT procedure for STM-4s	12-34
DFWT procedure for STM-16s	12-38

What to do if a DFWT fails on an optical port unit	12-42
DFWT procedure for electrical STM-1s	12-44
How to interpret which electrical STM-1 IU failed	12-48
What to do if a DFWT fails on an electrical STM-1	12-49
MD Inputs diagnostic test	
Overview	12-50
MD Inputs procedure	12-51
What to do if the MD Inputs diagnostic test fails	12-54
BSSU Optical Loopback diagnostic test	
Overview	12-55
BSSU Optical Loopback procedure	12-56
What to do if the Optical Loopback diagnostic test fails	12-60
STU Station Clock diagnostic test	
Overview	12-61
STU Station Clock procedure	12-62
What to do if the Station Clock diagnostic test fails	12-66
BSC, BSIU, BSSU, DTU, and STU Unit diagnostic tests	
Overview	12-67
BSC Unit procedure	12-68
BSIU and BSSU Unit procedure	12-71
DTU Unit procedure	12-74
STU Unit procedure	12-77
All other equipment diagnostic tests	
Overview	12-80
All other equipment diagnostic tests	12-81
What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails	12-84

What to do if the Network Interface test fails	12-85
What to do if the MCLAN diagnostic test fails	12-86
Diagnostic Testing - Test Results window	
Overview	12-87
Diagnostic Testing - Test Results window description	12-88
Test Results for the Device column description	12-89
Diagnostic Testing - Test Results	
Overview	12-90
Byte descriptions for equipment diagnostic tests	12-91
Test codes	12-93
Failure codes	12-103
Error codes	12-106

13 Execute alarm indicator, LED, and button tests

Overview	13-1
Background information	
Overview	13-2
Alarm indicator test terms	13-3
LEDS on PTMs	13-4
Alarm Indicator Tests window and procedures	
Overview	13-5
Alarm Indicator Tests window description	13-6
Running an alarm indicator test	13-8
Proving the standby SRC can turn off an alarm indicator	13-10
What to do if an MC end-of-suite alarm indicator test fails	13-11
What to do if an MS or port subrack end-of-suite alarm indicator test fails	13-12
What to do if an MC rack-top alarm indicator test fails	13-13

What to do if an MS or port subrack rack-top alarm indicator test fails	13-14
What to do if a User Panel alarm indicator test fails	13-15
LED Tests window and procedures	
Overview	13-16
LED Tests window description	13-17
Running an LED test	13-18
What to do if a unit LED test fails	13-19
What to do if a User Panel LED test fails	13-20
Button Tests window and procedures	
Overview	13-21
Button Tests window description	13-22
Running a button test	13-23
Button Testing - Test Results window	13-24
Byte descriptions for button test	13-25
What to do if the button test fails	13-26

14 View test results

Overview	14-1
View Test Results window description	14-2
How to view completed test results	14-3
View Results query	14-4

15 Background tests

Overview	15-1
Where to view background tests	15-2
Background Tests window description	15-3
Displaying background tests in progress	15-4
Cancelling a background test	15-5

16 Clear test history

Overview	16-1
Clear Test History window description	16-2
Clearing test records	16-3

17 Automatic laser shutdown

Overview	17-1
About automatic laser shutdown	17-2
Restart modes	17-3
Automatic Laser Shutdown window description	17-4
Restarting a laser	17-5

18 Database backups

Overview	18-1
Backup Database window	18-2
Backing up the system database	18-3

19 Fibre assignments

Overview	19-1
Fibre Assignments window description	19-2
Fibre-optic cable assignments	19-3
Querying fibre-optic cable assignments	19-4
Fibre Assignments query results	19-5

20 Test access

Overview	20-1
Background information	
Overview	20-2

Getting started	20-3
Test access concepts	20-4
MONE mode	
Overview	20-6
About MONE mode	20-7
Establishing MONE mode	20-8
Disconnecting MONE mode	20-9
MONF mode	
Overview	20-10
About MONF mode	20-11
Establishing MONF mode	20-12
Disconnecting MONF mode	20-13
MONEF mode	
Overview	20-14
About MONEF mode	20-15
Establishing MONEF mode	20-16
Disconnecting MONEF mode	20-18
SPLTA mode	
Overview	20-20
About SPLTA mode	20-21
Establishing SPLTA mode	20-22
Disconnecting SPLTA mode	20-25
SPLTB mode	
Overview	20-27
About SPLTB mode	20-28
Establishing SPLTB mode	20-29
Disconnecting SPLTB mode	20-32

SPLTAB mode

Overview	20-34
About SPLTAB mode	20-35
Establishing SPLTAB mode	20-36
Disconnecting SPLTAB mode	20-41

SPLTE mode

Overview	20-44
About SPLTE mode	20-45
Establishing SPLTE mode	20-46
Disconnecting SPLTE mode	20-47

SPLTF mode

Overview	20-48
About SPLTF mode	20-49
Establishing SPLTF mode	20-50
Disconnecting SPLTF mode	20-51

SPLTEF mode

Overview	20-52
About SPLTEF mode	20-53
Establishing SPLTEF mode	20-54
Disconnecting SPLTEF mode	20-57

LOOPE mode

Overview	20-59
About LOOPE mode	20-60
Establishing LOOPE mode	20-61
Disconnecting LOOPE mode	20-62

LOOPF mode

Overview	20-63

About LOOPF mode	20-64
Establishing LOOPF mode	20-65
Disconnecting LOOPF mode	20-66

21 Alarm clearing

Overview	21-1

General alarm clearing

Overview	21-4
ESD caution	21-5
Alarm clearing sequence	21-6
General alarm clearing flowchart	21-7
General alarm clearing procedure	21-8

AUcAIS

Overview	21-9
AUcAIS description	21-10
Clearing AUcAIS alarms	21-11

AUcLOP

Overview	21-12
AUcLOP description	21-13
Clearing AUcLOP alarms	21-14

BCLANcEQ

Overview	21-15
BCLANcEQ description	21-16
Clearing BCLANcEQ alarms	21-17

BOOTcSW

Overview	21-18
BOOTcSW description	21-19

Clearing BOOTcSW alarms	21-20
CABLEcEQ	
Overview	21-21
CABLEcEQ description	21-22
CABLEcEQ addresses	21-23
Clearing CABLEcEQ alarms	21-24
CABLEcTIM	
Overview	21-26
CABLEcTIM description	21-27
Differences between CABLEcEQ and CABLEcTIM alarms	21-28
Clearing CABLEcTIM alarms	21-29
DCNcCAALOF	
Overview	21-30
DCNcCAALOF description	21-31
Clearing DCNcCAALOF alarms	21-32
DCNcMSNoNBR	
Overview	21-33
DCNcMSNoNBR description	21-34
Clearing DCNcMSNoNBR alarms	21-35
DCNcRSNoNBR	
Overview	21-36
DCNcRSNoNBR description	21-37
Clearing DCNcRSNoNBR alarms	21-38
DCNcREPAIR	
Overview	21-39
DCNcREPAIR description	21-40
Clearing DCNcREPAIR alarms	21-41

DEGcEQ

Overview	21-42
DEGcEQ description	21-43
Clearing DEGcEQ alarms	21-44

DISKcFULL

Overview	21-45
DISKcFULL description	21-46
Clearing DISKcFULL alarms	21-47

FLTcEQ

Overview	21-48
FLTcEQ description	21-50
Clearing a FLTcEQ on an ARU, LHU, or PSP	21-51
Flowchart for clearing a FLTcEQ on a BSC or STU	21-52
Clearing a FLTcEQ on a BSC or STU	21-53
Flowchart for clearing a FLTcEQ on a BSIU or BSSU	21-56
Clearing a FLTcEQ on a BSIU or BSSU	21-57
Flowchart for clearing a FLTcEQ on a DTU	21-60
Clearing a FLTcEQ on a DTU	21-61
Flowchart for clearing a FLTcEQ on a fan in the MC subrack	21-63
Clearing a FLTcEQ on a fan in the MC subrack	21-64
Clearing a FLTcEQ on an IU or an unprotected port unit	21-67
Clearing a FLTcEQ on an MPU	21-69
Clearing a FLTcEQ on an MSU	21-70
Flowchart for clearing a FLTcEQ on an OLU	21-71
Clearing a FLTcEQ on an OLU	21-72
Flowchart for clearing a FLTcEQ on an SRC	21-74
Clearing a FLTcEQ on an SRC	21-75

Flowchart for clearing a FLTcEQ on an STM-1 electrical unit that uses 1:8 equipment protection	21-76
Clearing a FLTcEQ on an STM-1 electrical unit that uses 1:8 equipment protection	21-77
Flowchart for clearing a FLTcEQ on a port unit that uses NTT MSP	21-80
Clearing a FLTcEQ on a port unit that uses NTT MSP	21-81
Flowchart for clearing a FLTcEQ on a port unit that uses SNCP, ITU MSP, or ANSI MSP	21-84
Clearing a FLTcEQ on a port unit that uses SNCP, ITU MSP, or ANSI MSP	21-85
FLTcSW	
Overview	21-88
FLTcSW description	21-89
Clearing FLTcSW alarms for DUP cable problems	21-90
Clearing FLTcSW alarms on the MPU	21-91
Clearing FLTcSW alarms on the SRC	21-92
HPcDEG	
Overview	21-93
HPcDEG description	21-94
Clearing HPcDEG alarms	21-95
HPcPLM	
Overview	21-96
HPcPLM description	21-97
Clearing HPcPLM alarms	21-98
HPcRDI	
Overview	21-99
HPcRDI description	21-100
Clearing HPcRDI alarms	21-101

HPcTIM

Overview	21-102
HPcTIM description	21-103
Clearing HPcTIM alarms	21-104

HPcUNEQ

Overview	21-105
HPcUNEQ description	21-106
Clearing HPcUNEQ alarms	21-107

INTFcEQ

Overview	21-108
INTFcEQ description	21-109
INTFcEQ interfaces and addresses	21-110
Clearing INTFcEQ alarms	21-111

INVcCONF

Overview	21-112
INVcCONF description	21-113
Clearing INVcCONF alarms	21-114

INVcDPLL

Overview	21-115
INVcDPLL description	21-116
Clearing INVcDPLL alarms	21-117

INVcFPGA

Overview	21-119
INVcFPGA description	21-120
Clearing INVcFPGA alarms on a BSC, DTU, or STU	21-121
Clearing INVcFPGA alarms on port units	21-123

LPcDEG

Overview	21-124
LPcDEG description	21-125
Clearing LPcDEG alarms	21-126

LPcRDI

Overview	21-127
LPcRDI description	21-128
Clearing LPcRDI alarms	21-129

LPcTIM

Overview	21-130
LPcTIM description	21-131
Clearing LPcTIM alarms	21-132

LPcUNEQ

Overview	21-133
LPcUNEQ description	21-134
Clearing LPcUNEQ alarms	21-135

MCLANcEQ

Overview	21-136
MCLANcEQ description	21-137
MCLANcEQ flowchart	21-138
Clearing MCLANcEQ alarms	21-139

MDcIP{1–4}

Overview	21-141
MDcIP{1–4} description	21-142
Flowchart for clearing an MDcIP{1–4} alarm on a fan in a port rack	21-143
Clearing an MDcIP{1–4} alarm on a fan in a port rack	21-144

MScAIS

Overview	21-146
MScAIS description	21-147
Clearing MScAIS alarms	21-148

MScDEG

Overview	21-149
MScDEG description	21-150
Clearing MScDEG alarms	21-151

MScFOP

Overview	21-152
MScFOP description	21-153
Clearing MScFOP alarms	21-154

MScRDI

Overview	21-155
MScRDI description	21-156
Clearing MScRDI alarms	21-157

OOScSW

Overview	21-158
OOScSW description	21-159
Clearing OOScSW alarms	21-160

POWcDEG

Overview	21-161
POWcDEG description	21-162
Battery power	21-163
Clearing POWcDEG alarms	21-164

RScLOF

Overview	21-166

RScLOF description	21-167
Clearing RScLOF alarms	21-168
STMcLOS	
Overview	21-169
STMcLOS description	21-170
Clearing STMcLOS alarms	21-171
SYNCcCCRF	
Overview	21-172
SYNCcCCRF description	21-173
Possible causes of a SYNCcCCRF alarm	21-174
SYNCcCCRF flowchart	21-175
Clearing SYNCcCCRF alarms	21-176
SYNCcLTRF	
Overview	21-178
SYNCcLTRF description	21-179
SYNCcLTRF flowchart	21-180
Clearing SYNCcLTRF alarms	21-182
SYNCcROOR	
Overview	21-184
SYNCcROOR description	21-185
Clearing SYNCcROOR alarms	21-186
SYNCcSCF	
Overview	21-187
SYNCcSCF description	21-188
Clearing SYNCcSCF alarms	21-189
SYNCcSCHO	
Overview	21-190

SYNCcSCHO description	21-191
Clearing SYNCcSCHO alarms	21-192
SYNCcSTCOF	
Overview	21-193
SYNCcSTCOF description	21-194
SYNCcSTCOF flowchart	21-195
Clearing SYNCcSTCOF alarms	21-196
SYNCcSTCRF	
Overview	21-198
SYNCcSTCRF description	21-199
Clearing SYNCcSTCRF alarms	21-200
TEMPcEQ	
Overview	21-201
TEMPcEQ description	21-202
Clearing TEMPcEQ alarms	21-203
TUcAIS	
Overview	21-204
TUcAIS description	21-205
Clearing TUcAIS alarms	21-206
TUcLOM	
Overview	21-207
TUcLOM description	21-208
Clearing TUcLOM alarms	21-209
TUcLOP	
Overview	21-210
TUcLOP description	21-211
Clearing TUcLOP alarms	21-212

UNICeQ

Overview	21-213
UNICeQ description	21-214
Clearing UNICeQ alarms for most cases	21-215
Clearing UNICeQ alarms when the alarm appears after SRC insertion	21-216
Clearing UNICeQ alarms when the alarm is raised against a BSSU	21-217

VOLcDI

Overview	21-218
VOLcDI description	21-219
Clearing VOLcDI alarms	21-220

VOLcREP

Overview	21-221
VOLcREP description	21-222
Clearing VOLcREP alarms	21-223

WUPcEQ

Overview	21-224
WUPcEQ description	21-225
WUPcEQ flowchart	21-226
Clearing WUPcEQ alarms for SRC units	21-227
Clearing WUPcEQ alarms for all units except SRC units	21-228

22 Product warranty and repair

Overview	22-1
Product warranty	22-2
Product repair guidelines	22-4

Procedure for returning defective equipment

22-5

GL **Glossary**

GL-1

IN **Index**

IN-1



About this information product

Purpose This document contains all *WaveStar*[™] DACS 4/4/1 post-installation maintenance procedures.

What you need to know

You should have a basic understanding of Synchronous Digital Hierarchy (SDH) signalling before you attempt to use any of the procedures in this guide.

Reason for reissue The following features were added in Release 3.0 of *WaveStar* DACS 4/4/1:

- The addition of fans to port racks that are equipped with a PSC subrack
- The ability to connect the fan tray in a port rack to a Miscellaneous Discrete Input for fan failure alarm indications

The following feature was added in Release 3.1 of *WaveStar* DACS 4/4/1:

- New alarms associated with the use of a Data Communication Network (DCN). These were not available in Release 3.0, and the new information only applies to Release 3.1.

Safety labels Some tasks contain an admonishment symbol. This symbol is used to draw attention to important information about the task. The symbol appears in the following form:

**CAUTION**

Indicates a hazard that will or can cause minor personal injury or property damage if not avoided.

Intended audience

The following is a list of customers who will use this guide:

- Equipment engineers, including outside plant engineers
- Installation, operation, and maintenance personnel
- Switching office personnel
- System administrators
- Technical support personnel
- Training personnel

The following is a list of Lucent Technologies personnel who will use this guide:

- Developers
- System engineers
- System testers
- Sales support personnel
- Installation and engineering personnel
- Technical Support Organization
- Training personnel

Conventions used

The following conventions are used in this guide:

- Keys that you press are shown as **ENTER**.
- Text that is displayed on the screen is shown as `Unit provisioned and initialised.`
- Punctuation (such as periods and commas) are omitted when the user could mistake them as input. For example; Press **ENTER**
- Text that you enter is shown as `pboot 0 0`.
- Braces {} specify a range of possible entries, such as `PSA-{4–11, 4–19}`.
- Words that require emphasis are shown as *emphasis*.

Related documentation

The *WaveStar* DACS 4/4/1 set of documents includes the following:

Document title	Ordering number
<i>WaveStar</i> DACS 4/4/1 Application and Planning Guide	365-367-500
<i>WaveStar</i> DACS 4/4/1 Provisioning Guide	365-367-512
<i>WaveStar</i> DACS 4/4/1 Quick Reference Card	365-367-503
Integrated Transport Management Sub-network Controller (ITM-SC) Sub-network Provisioning Guide (SPG) for <i>WaveStar</i> DACS 4/4/1	190-223-151

Related training Lucent Technologies provides the following *WaveStar* DACS 4/4/1 training courses:

- DG3404 — Overview
- TR3562 — Administration, Provisioning, and Maintenance

For up-to-date training information, see <http://www.lucent-product-training.com/SabaWeb>.

How to order The ordering number for this document is 365-367-513.

If you order by mail, address your request to:

Lucent Technologies Customer Information Center

Attention: Order Entry Section

2855 N. Franklin Road

P.O. Box 19901

Indianapolis, Indiana, U.S.A. 46219

If you order by phone from the United States, call:

1-888-582-3688

FAX: +1-800-566-9568

If you order by phone from outside the United States, call:

+1-317-322-6416

FAX: +1-317-322-6699

A check, money order, purchase order number, or charge number VISA bank card, American Express card services, or MasterCard bank card is required with all orders. Make checks payable to Lucent Technologies.



1 Product description

Overview

Purpose “Product description” provides a high-level description of the *WaveStar*[™] DACS 4/4/1.

Organisation “Product description” is organised as follows:

- “System description” (1-2)
- “Equipment description” (1-10)



System description

Overview

Purpose This section provides a high-level description of the system.

Organisation This section is organised as follows:

- “System description” (1-3)
- “System capacity” (1-5)
- “Control system” (1-6)
- “System interfaces” (1-8)
- “Synchronisation and timing” (1-9)



System description

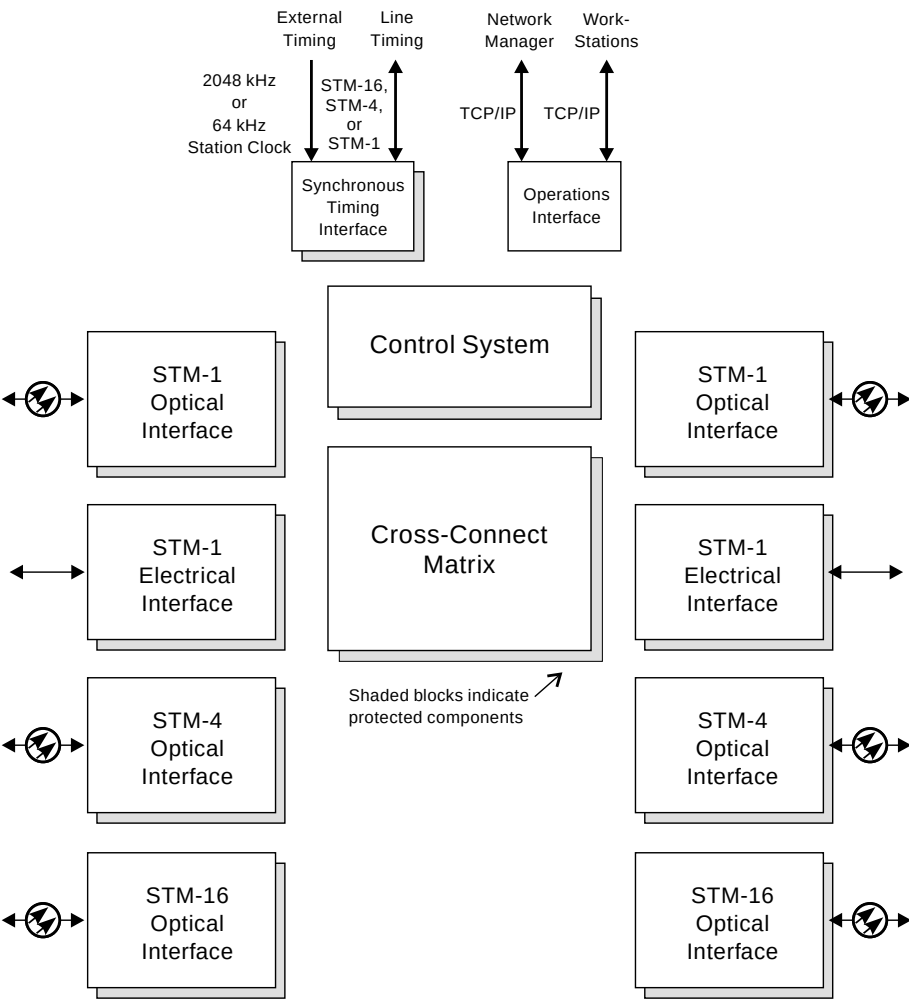
Functional description

The system is a large-capacity cross-connect system that provides flexible bandwidth management in a Synchronous Digital Hierarchy (SDH) environment. The system can be equipped with various transmission interfaces, and supports cross connections at broadband and wideband rates.

The system has a nonblocking, full-broadcast cross-connect matrix. The cross-connect matrix is compatible with both American National Standards Institute (ANSI) and International Telecommunications Union (ITU) transmission standards and is capable of cross connecting all tributaries defined by them.

The cross-connect matrix and all internal transmission paths are fully protected by a 2:8 protection architecture. This architecture provides triple protection, resulting in very high availability. High availability is important, because a large cross-connect system carries an immense amount of traffic.

The following illustration shows a block diagram of the system.



□

System capacity

Available system configurations

The system can be configured for a maximum capacity of either 256 STM-1 equivalents or 512 STM-1 equivalents. The system capacity determines the number of port subracks that can be provisioned.

Differences between 256 and 512 systems

The differences between 256 and 512 STM-1 equivalent systems are as follows:

- A 256 STM-1 equivalent system can have a maximum of eight port subracks.
- A 512 STM-1 equivalent system can have a maximum of 16 port subracks.

Displaying the maximum system capacity

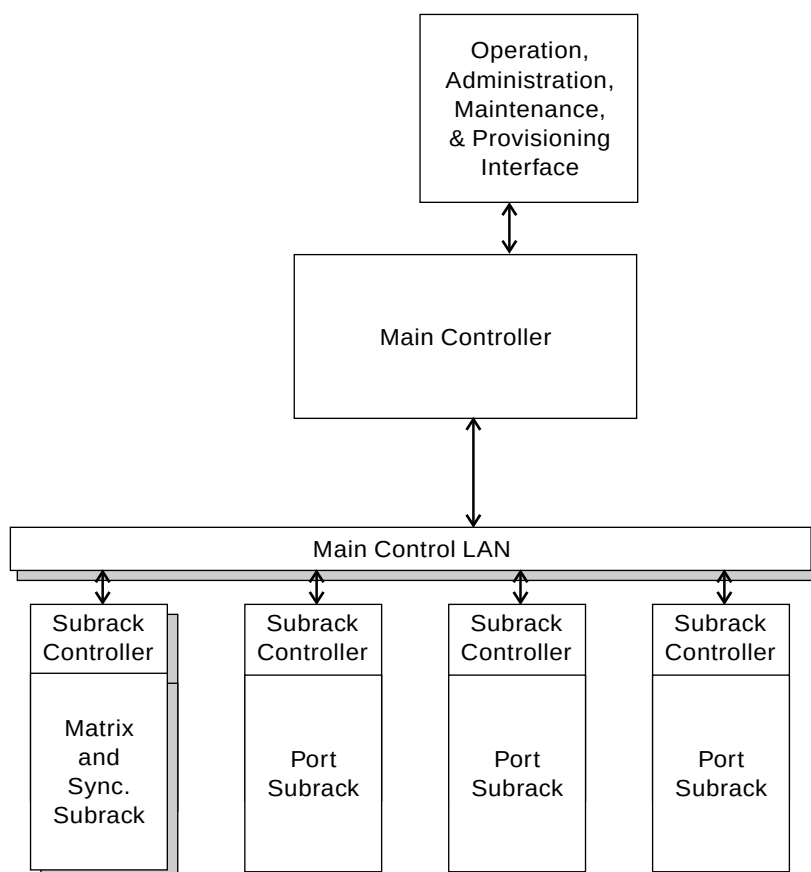
To display the maximum system capacity, go to *Help > About....*



Control system

Overview System coordination and control is carried out by the Main Controller, the subrack controllers, and the board controllers.

Illustration The following illustration shows a block diagram of the control structure.



Main Controller The Main Controller (MC) provides local and remote interfaces for operations, administration, maintenance, and provisioning. The MC accepts commands from these interfaces and translates them into equipment level instructions that are sent to the subrack controllers.

New software releases can be loaded onto the MC without interrupting service.

A duplicated MC is available. The primary purpose of a duplicated MC is to increase system availability. The second (standby) MC takes control of the system if the active MC fails.

Subrack controllers Subrack controllers route messages to and from the Main Controller and the board controllers.

Board controllers Board controllers perform control processing for most types of units. Functions performed by board controllers include executing commands received from subrack controllers and sending maintenance or performance data to subrack controllers.



System interfaces

- Network interfaces** This release provides the following Synchronous Digital Hierarchy (SDH) network interfaces:
- STM-16 long-haul optical designed to ITU specifications
 - STM-4 short-haul optical designed to ITU specifications
 - STM-1 long-haul optical designed to ITU specifications
 - STM-1 short-haul optical designed to ITU specifications
 - STM-1 short-haul optical designed to Nippon Telegraph and Telephone (NTT) specifications
 - STM-1 electrical
- 1:8 equipment protection is available for STM-1 electrical interfaces. 1+1 Multiplex Section Protection (MSP) and Sub-Network Connection Protection (SNCP) are available for all transmission interfaces.
- OAM&P interfaces** Operations, Administration, Maintenance, and Provisioning (OAM&P) activities can be performed locally from a PC with XC-CIT application software, from a remote V.28 dial-up connection, or from a remote network or element management system. All OAM&P connections use Transmission Control Protocol/Internet Protocol (TCP/IP).



Synchronisation and timing

Synchronisation and timing capabilities

The system has duplicated synchronisation and timing hardware that provides the following capabilities:

- The System Timing Unit (STU) has an ITU G.812 Type I clock with holdover mode.
- System clock input references can be derived from transmission ports, including ports that are provisioned for MSP or SNCP, or from external references (station clock inputs).
- External references can be derived from 2048 kHz inputs or from 64 kHz composite clock inputs.
- Reference source and timing mode selection are based on user-assigned priorities.
- System timing is distributed to transmission hardware within the system.
- Each STU has a 2048 kHz station clock output port that can be used as a timing source for other equipment.
- When no faults are present, user-initiated protection switching of the synchronisation and timing hardware is glitchless.



Equipment description

Overview

Purpose This section describes the system racks, subracks, and units.

Organisation This section is organised as follows:

- [“Equipment terms” \(1-11\)](#)
- [“Matrix and Synchronisation rack” \(1-12\)](#)
- [“Matrix and Synchronisation subrack” \(1-13\)](#)
- [“Bit Slice Switch Unit \(BSSU\)” \(1-15\)](#)
- [“Matrix and Control rack” \(1-16\)](#)
- [“Main Controller subrack” \(1-17\)](#)
- [“User Panel” \(1-20\)](#)
- [“Alarm Connector Panel \(ACP\)” \(1-22\)](#)
- [“Fan Connector Panel \(FCP\)” \(1-25\)](#)
- [“Port rack” \(1-27\)](#)
- [“Port Subrack A \(PSA\)” \(1-28\)](#)
- [“Port Subrack C \(PSC\)” \(1-30\)](#)
- [“Port rack fan tray connector panel” \(1-32\)](#)



Equipment terms

List of terms

Rack A rack is a mechanical assembly that houses the system equipment. A rack can be equipped with one or two subracks. All racks conform to European Telecommunications Standards Institute (ETSI) equipment practices for transmission products.

Subrack A subrack is a mechanical assembly that houses plug-in units, also referred to as circuit packs. All subracks conform to ETSI equipment practices for transmission products. All subracks have a midplane that interconnects the units in the subrack and partitions the subrack into front and rear sections. A unit plugs into either the front or the back of a subrack.

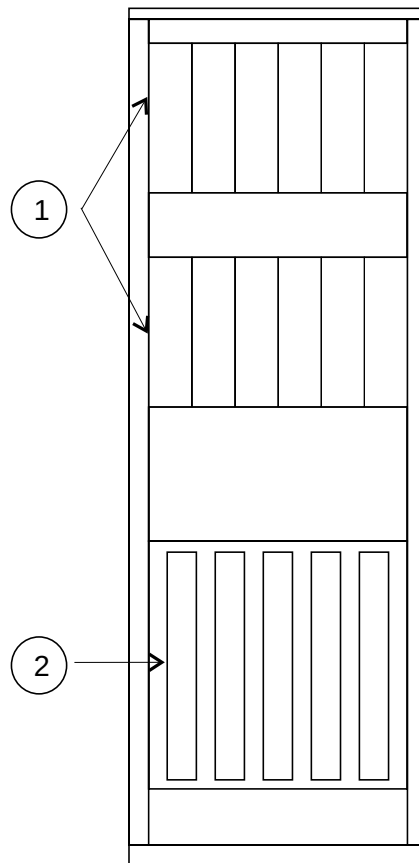
Unit A unit contains the circuitry for the system. It plugs into either the front or the back of a subrack. A unit is also called a plug-in, a circuit pack, or a pack.



Matrix and Synchronisation rack

Description The Matrix and Synchronisation rack is an ETSI standard rack that houses the Matrix and Synchronisation subrack and five Bit Slice Switch Units (cross-connect matrix components).

Illustration The following illustration shows a front view of the Matrix and Synchronisation rack with the doors removed.



Legend:

1. Matrix and Synchronisation subrack with duplicated Matrix Control and Synchronisation hardware
2. Bit Slice Switch Units (BSSUs)



Matrix and Synchronisation subrack

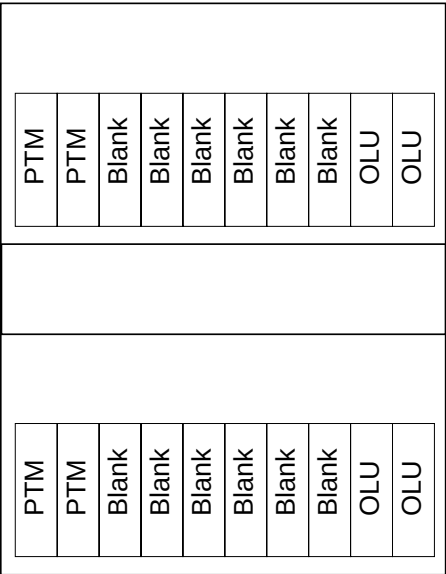
Description The Matrix and Synchronisation subrack has two shelves with front and rear sections that are partitioned for plug-in units (circuit packs). Each shelf is equipped with the same set of matrix control and synchronisation and timing hardware. The units plug into a midplane that separates the front and rear sections and provides the interconnections between units.

Illustration, front view The following illustration shows a front view of the Matrix and Synchronisation subrack.

STU	BSC	Blank	Blank	Blank	SRC
STU	BSC	Blank	Blank	Blank	SRC

- Units, front of subrack** The following units plug into the front of the Matrix and Synchronisation subrack:
- The System Timing Unit (STU) provides system timing and synchronisation.
 - The Bit Slice Controller (BSC) works with the STU to provide timing signals for internal transmission paths. The BSC also provides control information for the Bit Slice Switch Units (BSSUs).
 - The Subrack Controller (SRC) routes messages back and forth from the Main Controller to the units in the Matrix and Synchronisation subrack.

Illustration, rear view The following illustration shows a rear view of the Matrix and Synchronisation subrack.



Units, back of subrack The following units plug into the back of the Matrix and Synchronisation subrack:

- The Power Terminal Module (PTM) filters incoming station power from two separate power sources and distributes it across the midplane.
- The Optical Link Unit (OLU) is part of the internal transmission path. It provides interfaces for the optical-fibre cables that carry transmission data between the BSCs and the BSSUs. The OLU also provides interfaces for the optical-fibre cables that carry timing information between the duplicated BSCs in the Matrix and Synchronisation subrack.



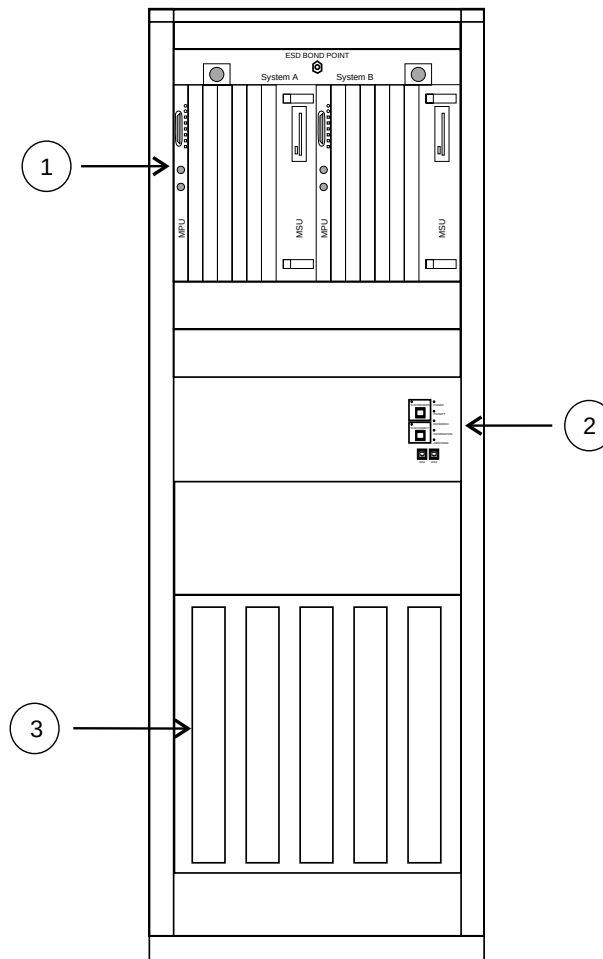
Bit Slice Switch Unit (BSSU)

Description	The Bit Slice Switch Units (BSSUs) are cross-connect matrix components. The system has ten BSSUs. Five BSSUs are located in the bottom of the Matrix and Synchronisation rack, and five BSSUs are located in the bottom of the Matrix and Control rack.	☐

Matrix and Control rack

Description The Matrix and Control rack is an ETSI standard rack that houses the Main Controller subrack, User Panel, and five BSSUs (cross-connect matrix components).

Illustration The following illustration shows a front view of the Matrix and Control rack with the doors removed.



Legend:

1. Main Controller (MC) subrack with a duplicated Main Controller
2. User Panel
3. Bit Slice Switch Units (BSSUs)

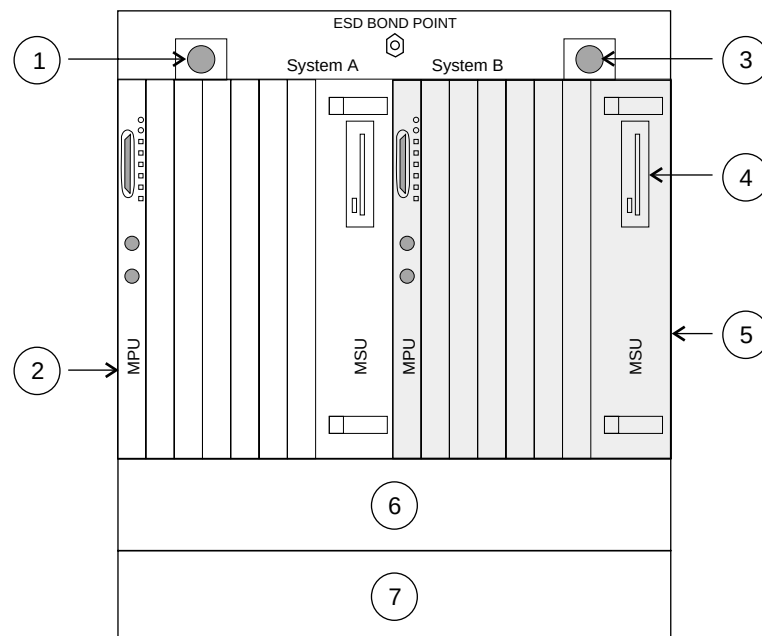


Main Controller subrack

Description The Main Controller (MC) subrack has a card cage, a fan tray, and a power supply. The card cage has front and rear sections that are partitioned for plug-in units and transition modules. The units and transition modules plug into a midplane that separates the front and rear sections of the card cage and provides the interconnections between units and transition modules.

A duplicated MC is available. When the MC is duplicated, the system automatically switches to the standby MC if the active MC fails.

Illustration, front view The following illustration shows a front view of the Main Controller subrack with a duplicated MC.



Legend:

1. Power button for the working MC
2. Working MC
3. Power button for the protection MC
4. Magneto Optical (MO) disk drive
5. Protection MC (shaded area)
6. Fan tray
7. Power supply

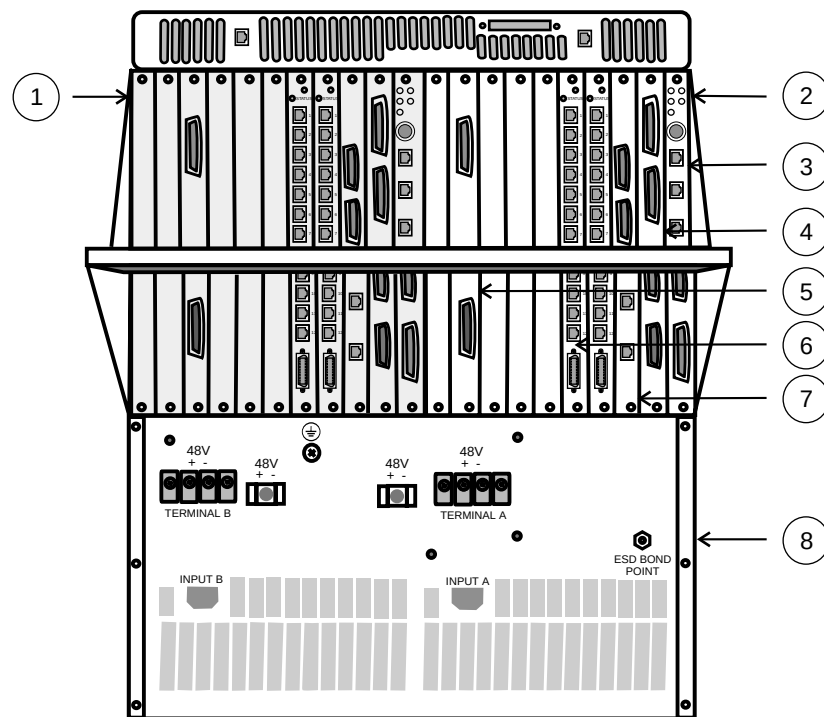
Units, front of subrack

The following units plug into the front of the Main Controller subrack:

- The Main Processor Unit (MPU) provides the central processing function, which includes control of the ARU, LHU, and MSU.
- The Mass Storage Unit (MSU) contains a fixed-medium hard disk drive and a removable-medium optical disk drive.

Illustration, rear view

The following illustration shows a rear view of the Main Controller subrack with a duplicated MC.



Legend:

1. Protection MC (shaded area)
2. Working MC
3. ARU
4. Serial TM
5. SCSI TM
6. LHU
7. NIC TM
8. Fans and power supply

Units, back of subrack

The following units and transition modules (TMs) plug into the back of the Main Controller subrack:

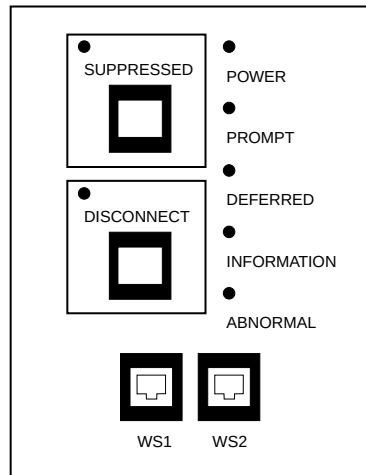
- The Alarm Relay Unit (ARU) provides interfaces to system alarm indicators, a network interface to the LHU, and a narrow Small Computer System Interface-2 (SCSI-2) to the MSU.
- The LHUs provide the hub ports for system LAN connections.
- The Network Interface Chip (NIC) Transition Module provides LAN access to the MPU.
- The Small Computer System Interface (SCSI) Transition Module provides a narrow SCSI-2 interface between the MPU and the MSU.
- The Serial Transition Module provides serial I/O access to the MPU.



User Panel

Description The User Panel is located below the Main Controller subrack. The User Panel provides general system status and alarm information.

Illustration The following illustration shows a front view of the User Panel.



Components The User Panel has the following alarm indicators, switches, and connectors:

- The POWER LED is not used in this release.
- PROMPT is a red LED that indicates that an alarm classified as prompt exists in the system.
- DEFERRED is a red LED that indicates that an alarm classified as deferred exists in the system.
- INFORMATION is a yellow LED that indicates that an alarm classified as information exists in the system.
- The ABNORMAL LED is not used in this release.

- SUPPRESSED and DISCONNECT are push-button switches that enable users to suppress or disconnect alarm indications. The yellow LED next to the SUPPRESSED switch indicates that alarm indications are suppressed. The yellow LED next to the DISCONNECT switch indicates that alarm indications are disconnected.
- WS1 and WS2 are V.28 DCE 8-pin modular connectors. WS1 is used to connect a terminal or a modem to the working Main Controller for local or remote operations, administration, maintenance, and provisioning activities. WS2 is used to connect a terminal or a modem to the protection Main Controller for local or remote operations, administration, maintenance, and provisioning activities. WS2 can be used only if the system has a duplicated Main Controller.



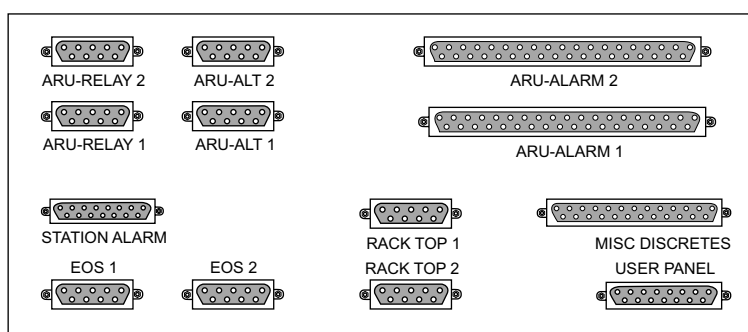
Alarm Connector Panel (ACP)

Description The Alarm Connector Panel (ACP) is located on the back of the User Panel. The ACP has connectors for alarm-related cables.

The ACP provides alarm signal routing from the ARU to the following:

- User Panel
- Other system and customer-provided and designed alarm panels

Illustration The following illustration shows a front view of the Alarm Connector Panel.



Components The Alarm Connector Panel has the following components:

- ARU-RELAY 1 is a DB-9 female connector. The other end of the cable that attaches to this connector attaches to the connector labeled ALM RMT on the ARU in Main Controller 1 (MC-1). This interface carries station alarm signals from the ARU to the ACP.
- ARU-RELAY 2 is a DB-9 female connector. The other end of the cable that attaches to this connector attaches to the connector labeled ALM RMT on the ARU in MC-2. This interface carries station alarm signals from the ARU to the ACP. The ARU-RELAY 2 connector is used only if the system has a duplicated MC.
- ARU-ALT 1 is a DB-9 female connector. The other end of the cable that attaches to this connector attaches to the connector labeled ALM/IO on the ARU in MC-1. This interface carries User Panel alarm signals, for example, system-level Prompt, Deferred, and Information alarm signals, from the ARU to the ACP.

- The ARU-ALT 2 is a DB-9 female connector. The other end of the cable that attaches to this connector attaches to the connector labeled ALM/IO on the ARU in MC-2. This interface carries User Panel alarm signals, for example, system-level Prompt, Deferred, and Information alarm signals, from the ARU to the ACP. The ARU-ALT 2 connector is used only if the system has a duplicated MC.
- ARU-ALARM 1 is a DB-37 female connector. The other end of the cable that attaches to this connector attaches to the connector labeled ALARM/IO on the ARU in MC-1. This interface carries Rack Top, End-Of-Suite, and Miscellaneous Discrete alarm signals from the ARU to the ACP.
- ARU-ALARM 2 is a DB-37 female connector. The other end of the cable that attaches to this connector attaches to the connector labeled ALARM/IO on the ARU in MC-2. This interface carries Rack Top, End-Of-Suite, and Miscellaneous Discrete alarm signals from the ARU to the ACP. The ARU-ALARM 2 connector is used only if the system has a duplicated MC.
- STATION ALARM is a DB-15 female connector. This connector provides an interface for customer-provided and designed station alarm indicators.
- EOS 1 is a DB-9 female connector. This connector provides an interface for customer-provided and designed End-of-Suite alarm indicators.
- EOS 2 is a DB-9 female connector. This connector provides an interface for customer-provided and designed End-of-Suite alarm indicators. The EOS 2 connector is used only if the system has a duplicated MC.
- RACK TOP 1 is a DB-9 female connector. This connector provides an interface for the rack-top alarm indicators on the Matrix and Control rack, and a power sense lead that indicates loss of input power to the MC.
- RACK TOP 2 is a DB-9 female connector. This connector provides an interface for the rack-top alarm indicators on the Matrix and Control rack, and a power sense lead that indicates loss of input power to the MC. The RACK TOP 2 connector is used only if the system has a duplicated MC.

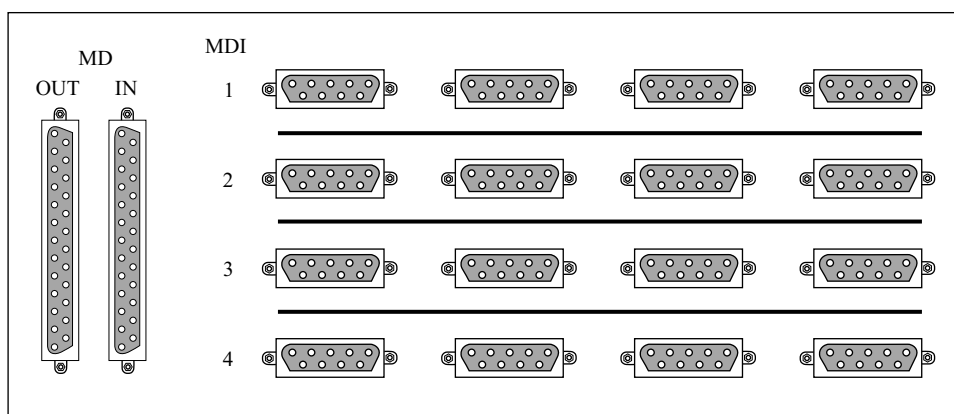
- MISC DISCRETES is a DB-25 female connector. The other end of the cable that attaches to this connector attaches to the connector labeled MD OUT on the FCP. This connector provides an interface for miscellaneous customer-provided and designed alarm indicators or other applications.
- USER PANEL is a DB-15 female connector. The other end of the cable that attaches to this connector is permanently connected to the User Panel.



Fan Connector Panel (FCP)

Description The Fan Connector Panel (FCP) is located on the back of the User Panel. The FCP has connectors for alarm-related cables, and routes alarm signals from fan trays in port racks equipped with PSC subracks and from customer-provided and designed alarm panels to the ACP.

Illustration The following illustration shows a front view of the Fan Connector Panel.



Components The Fan Connector Panel has the following components:

- MD OUT is a DB-25 female connector. The other end of the cable that attaches to this connector attaches to the connector labeled MISC DISCRETES on the ACP. This connector provides an interface from miscellaneous customer-provided and designed alarm indicators or other applications to the ACP.
- MD IN is a DB-25 female connector. The other end of the cable that attaches to this connector attaches to customer-provided and designed alarm indicators or other applications. This connector provides an interface for miscellaneous customer-provided and designed alarm indicators or other applications.
- MDI 1 through 4 are DB-9 female connectors. The other end of the cable that attaches to each of these connectors attaches to the connector labeled ALM on the fan tray connector panel in each port rack that is equipped with a PSC subrack. This interface carries alarm signals from the port rack fan tray to the FCP.

□

Bit Slice Switch Unit (BSSU)

Description The Bit Slice Switch Units (BSSUs) are cross-connect matrix components. The system has ten BSSUs. Five BSSUs are located in the bottom of the Matrix and Synchronisation rack, and five BSSUs are located in the bottom of the Matrix and Control rack.



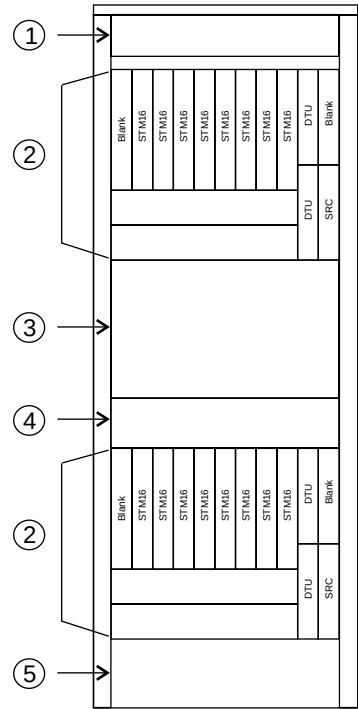
Port rack

Description The port rack is an ETSI standard rack. It can be equipped with one or two PSA subracks, one or two PSC subracks, or one PSA subrack and one PSC subrack. The PSB subrack, for STM-0 interfaces, has been discontinued.

Port racks that are equipped with one or two PSC subracks are also equipped with a fan tray, heat duct, and bottom filter tray. The fan tray is located in the middle of the port rack and contains six fans, fan filters, and a connector panel. Refer to “Port rack fan tray connector panel” (1-32) for a description of the fan tray connector panel.

When a port rack is equipped with only one PSC subrack, the subrack must be located in the bottom of the port rack.

Illustration The following illustration shows a front view of a port rack with the doors removed. The port rack is equipped with two PSC subracks.



- Legend:**
- 1. Power and fuse panel
 - 2. PSC subrack
 - 3. Heat duct
 - 4. Fan tray and filters
 - 5. Bottom filter tray



Port Subrack A (PSA)

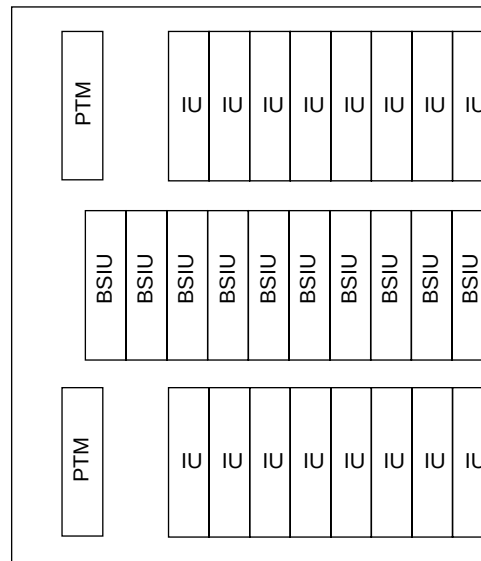
Description The Port Subrack A (PSA) has front and rear sections that are partitioned for plug-in units. The PSA can be equipped with any combination of STM-1 port units and interface units. The units plug into a midplane that separates the front and rear sections and provides the interconnections between units.

Illustration, front view The following illustration shows a front view of the PSA subrack.

STM1	STM1	STM1	STM1	STM1	STM1	STM1	STM1	STM1 P	DTU	Blank
STM1	STM1	STM1	STM1	STM1	STM1	STM1	STM1	STM1 P	DTU	SRC

- Units, front of subrack** The following units plug into the front of the PSA subrack:
- STM-1 Port Unit (STM-1) — The STM-1 port unit provides four STM-1 (155.52 Mbps) ports. The STM-1 P is the protection unit for a shelf that is configured for 1:8 equipment protection.
 - Digital Timing Unit (DTU) — The DTU provides timing for the transmission units in the subrack. The DTU is always duplicated.
 - Subrack Controller (SRC) — The SRC routes messages back and forth from the Main Controller to the units in the port subrack.

Illustration, rear view The following illustration shows a rear view of the PSA subrack.



Units, back of subrack The following units plug into the back of the PSA subrack:

- Power Terminal Module (PTM) — The PTM filters incoming station power from two separate power sources and distributes it across the midplane.
- Bit Slice Interface Unit (BSIU) — The BSIU is part of the transmission path. It transports data between the BSSUs (cross-connect matrix components) and the port units. The BSIU also monitors the transmission data and provides automatic protection switching for hardware failures.
- STM-1 Interface Unit (IU) — The STM-1 interface unit provides the SDH Physical Interface (SPI) function for STM-1 electrical and optical signals. All STM-1 interface units work with the STM-1 port unit.

The following STM-1 IUs are available:

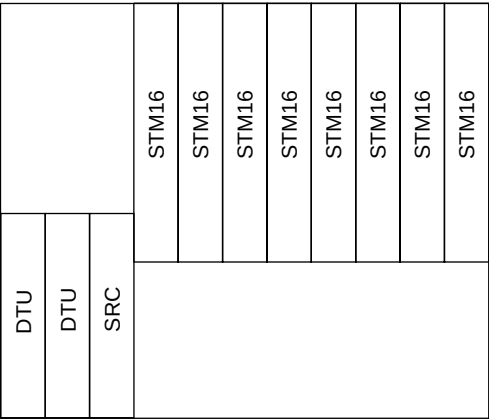
- STM-1 electrical interface unit
- STM-1 short-haul optical interface unit designed to ITU specifications
- STM-1 long-haul optical interface unit designed to ITU specifications
- STM-1 short-haul optical interface unit designed to Nippon Telegraph and Telephone (NTT) specifications

□

Port Subrack C (PSC)

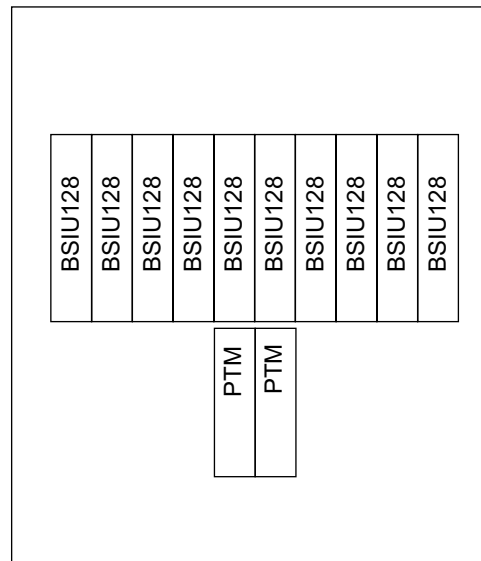
Description The Port Subrack C (PSC) has front and rear sections that are partitioned for plug-in units. The PSC can be equipped with STM-16 or STM-4 port units. For this release, a PSC cannot be equipped with a combination of STM-16 and STM-4 port units. The units plug into a midplane that separates the front and rear sections and provides the interconnections between units.

Illustration, front view The following illustration shows a front view of the PSC subrack.



- Units, front of subrack** The following units plug into the front of the PSC subrack:
- STM-16 Port Unit (STM-16) — The STM-16 port unit has one STM-16 port. The STM-16 port provides 2.5 Gbit/s transmission.
 - STM-4 Port Unit (STM-4) — The STM-4 port unit has four STM-4 ports. Each STM-4 port provides 622 Mbit/s transmission.
 - Digital Timing Unit (DTU) — The DTU provides timing for the transmission units in the subrack. The DTU is always duplicated.
 - Subrack Controller (SRC) — The SRC routes messages back and forth from the Main Controller to the units in the port subrack.

Illustration, rear view The following illustration shows a rear view of the PSC subrack.



Units, back of subrack The following units plug into the back of the PSC subrack:

- Power Terminal Module (PTM) — The PTM filters incoming station power from two separate power sources and distributes it across the midplane.
- Bit Slice Interface Unit (BSIU) 128 — The BSIU128 is part of the internal transmission path. It transports data between the BSSUs (cross-connect matrix components) and the port units. The BSIU128 also monitors the transmission data and provides Automatic Protection Switching for hardware failures. The BSIU128s in the PSC subrack can transport twice the bandwidth, up to 128 STM-1 equivalents, compared to the BSIUs in the PSA subrack, which can transport up to 64 STM-1 equivalents.



Port rack fan tray connector panel

Description The fan tray connector panel is located on the back of the fan tray in port racks that are equipped with a PSC subrack.

Components The port rack fan tray connector panel has the following components:

- ALM is a DB-9 female connector. The other end of the cable that attaches to this connector attaches to one of the Miscellaneous Discrete Input (MDI) connectors on the Fan Connector Panel (FCP). This interface carries alarm signals from the port rack fan tray to the FCP.
- PWR is a DB-3 male connector. The PWR connector terminates the cable that provides duplicated –48 volt power to the port rack fan tray.
- The FAIL LED is a red LED that lights when one or more fans in the port rack fan tray fail.





2 About units and disks

Overview

Purpose “About units and disks” contains information about the system units and disks, and the procedures for inserting and removing them.

Related topics

For information about system racks, subracks, and where a units are located, see [“Equipment description” \(1-10\)](#)

Organisation “About units and disks” is organised as follows:

- [“Background information” \(2-2\)](#)
- [“MO disks” \(2-6\)](#)
- [“Units in the MS or port subrack” \(2-10\)](#)
- [“ARUs, LHUs, and PSPs” \(2-15\)](#)
- [“MPUs and MSUs” \(2-20\)](#)
- [“Serial TM, NIC TM, and SCSI TM” \(2-24\)](#)
- [“Unit codes and spare equipment list” \(2-30\)](#)



Background information

Overview

Purpose This section contains background information about units.

Organisation This section is organised as follows:

- “Unit terms” (2-3)
- “About Electrostatic Discharge” (2-4)
- “Unit precautions” (2-5)



Unit terms

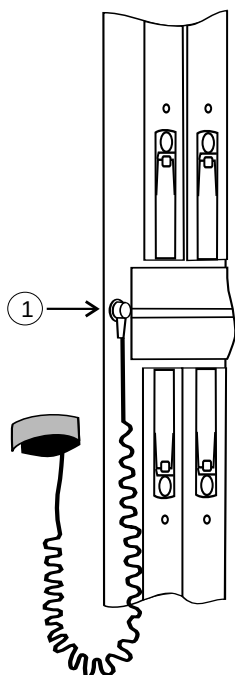
- List of terms**
- Electrostatic Discharge** Electrostatic Discharge (ESD) is the sudden release of the charge associated with static electricity. Static charge is generated whenever two materials come into contact with each other and are then separated.
- Magneto Optical disks** A Magneto Optical (MO) disk is a removable storage medium. MO disks are used for backing up the system database and for loading software onto the system.
- Unit** A unit is the hardware that is inserted into an equipment shelf. A unit is also called a plug-in, circuit pack, or pack.



About Electrostatic Discharge

- ESD precautions** This system contains integrated circuits and other electronic equipment that are sensitive to Electrostatic Discharge (ESD). Use the following guidelines to prevent equipment damage:
- Carefully remove any equipment that is shipped in special packing.
 - Assume that all electronic devices are sensitive to ESD.
 - Keep work areas clear of common plastic materials, since they are a major source of static electricity.

ESD wrist strap Before touching any system equipment, put on an ESD wrist strap and plug the wrist strap into an ESD jack. Every equipment rack has an ESD jack.



Legend:

1. ESD jack

ESD damage It is difficult to identify ESD damage, because in many cases you cannot see physical damage. Any static-sensitive device that has been exposed to ESD may function normally but may also have a reduced life expectancy, or the device may function erratically.



Unit precautions

Handling units

When handling units, keep the following precautions in mind:

- Before handling a unit, put on an ESD wrist strap and plug the wrist strap into an ESD jack.
- Never hand a unit to a person who is not wearing an ESD wrist strap that is connected to the system equipment.
- Keep units away from possible sources of static electricity, such as clothing and common plastics.
- Handle units only by the faceplate, latch, or by the top and bottom edges.
- Never touch the leads, connectors, or connector pins on a unit.
- Never attach gummed labels or tape to a unit.
- Use only approved cleaners for cleaning unit contacts.
- Observe warning labels on bags and cartons.
- Remove all jewellery to avoid shock and damage to both you and the equipment.
- Never remove more than one unit at a time.
- Call technical support before attempting to remove a unit from the Main Controller (MC) subrack.
- The BSSUs contain fluorinert, a liquid coolant. Do not open these units. Return BSSUs to the manufacturer for repair or disposal.



MO disks

Overview

Purpose This section contains information about Magneto Optical (MO) disks.

Organisation This section is organised as follows:

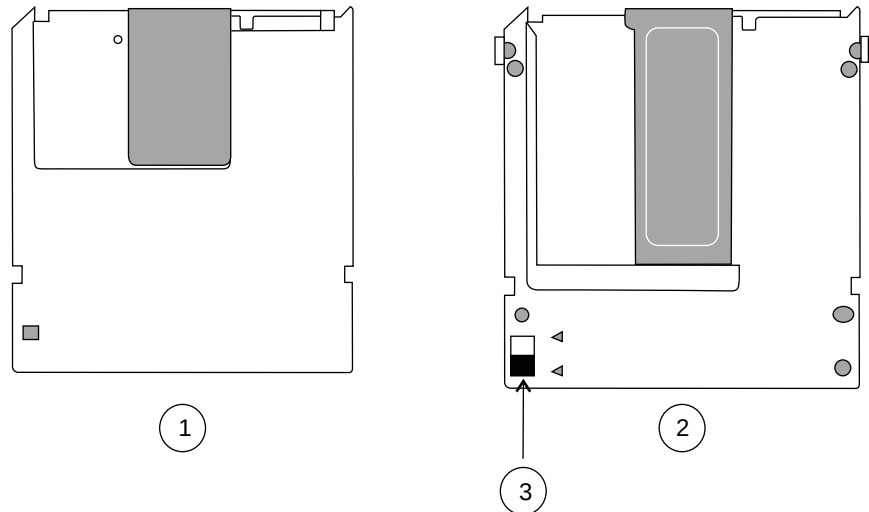
- “About MO disks” (2-7)
- “Inserting an MO disk” (2-8)
- “Removing an MO disk” (2-9)



About MO disks

Description of MO disks

Magneto Optical (MO) disks have a direction arrow on the top to assist in insertion and a write-protection slide on the bottom to protect recorded data. The write-protection slide is activated from the back side of the MO disk.

**Legend:**

- 1. Front
- 2. Back
- 3. Write protect slide

Disk capacity

An MO disk has a 4 gigabyte capacity.

MO disk storage

Store MO disks in a dust-free, low-humidity environment away from excessive heat, cold, and magnetism. Do not touch or allow external objects to touch exposed surfaces of the storage medium.



Inserting an MO disk

Procedure

- 1** Make sure that the write-protection slide on the Magneto Optical (MO) disk is in the proper position for the operation you want to perform.
 - Write enabled (labelled nonprotected or recordable on the disk) if you are going to write to or format this disk
 - Write protected (labelled protected or nonrecordable on the disk) if you are only going to read from this disk

- 2** Insert an MO disk into the MO disk drive located near the top of the MSU unit.

- 3** Position the disk so that the front faces the left side of the drive, and the arrow printed on the disk is on the bottom left side of the disk.

- 4** Slide the disk into the drive until the disk is inserted all the way and clicks into place.

END OF STEPS



Removing an MO disk

Procedure

- 1 Make sure that the drive is not active by verifying that the activity LED on the drive is not lit.
-

- 2 Press the disk release button on the front of the drive, and remove the disk.

If the rack has lost power, use the Optical Disk Ejection tool to remove the Magneto Optical (MO) disk.

END OF STEPS



Units in the MS or port subrack

Overview

Purpose This section contains information about units in the Matrix and Synchronisation or in a port subrack.

Organisation This section is organised as follows:

- “Removing a unit from the MS or port subrack” (2-11)
- “Inserting a unit into the MS or port subrack” (2-13)



Removing a unit from the MS or port subrack

Purpose The DACS system comes with units already installed. Perform the following procedure only if you need to remove a unit from the Matrix/Synchronisation subrack or from a port subrack.

Before you begin Perform the specific FLTcEQ unit-replacement procedure before you remove a unit.

Reference

For the unit-replacement procedures, see “FLTcEQ flowcharts and procedures” (21-48).



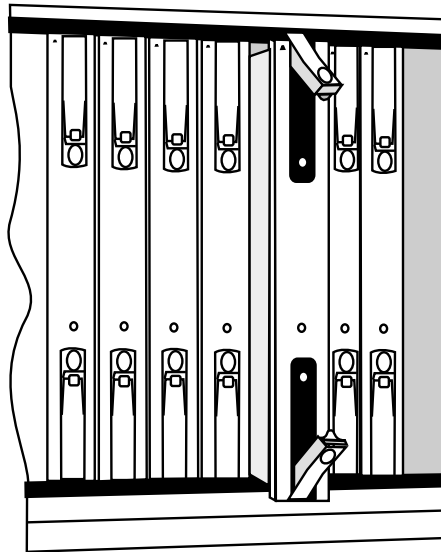
CAUTION

Never remove more than one unit at a time. Removing more than one unit at a time can cause damage to the units, the midplane, or both.

Procedure **Important!** You can damage units by improperly removing them. Read the entire procedure before removing a unit.

-
- 1 If cables are attached to the unit, remove the cables from the unit. If you plan to reattach the cables, label the cables so that you know where to reattach them.

-
- 2** Simultaneously open the install and remove latches at the top and bottom of the unit.



To open the install and remove latches, push up on the top latch and down on the bottom latch.



CAUTION

Pull evenly on both latches when you remove a unit. If you remove a unit unevenly, you may cause a temporary glitch to service.

- 3** While grasping the install and remove latches, pull *evenly* to slide the unit out of the subrack.

END OF STEPS



Inserting a unit into the MS or port subrack

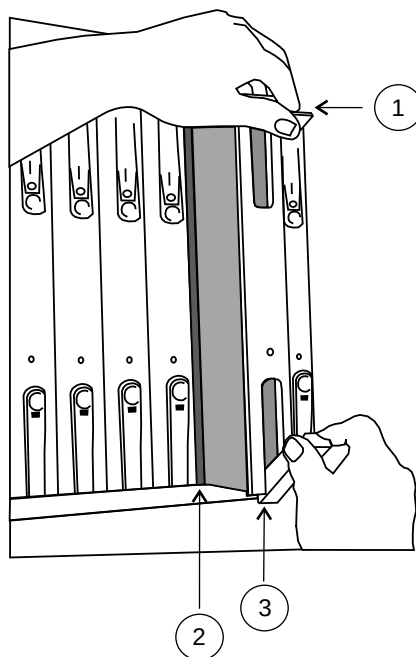
Procedure

- 1** Remove the plastic shipping protector from the contacts of the new unit.

- 2** Simultaneously open the install and remove latches at the top and bottom of the unit.

To open the install and remove latches, push up on the top latch and down on the bottom latch.

- 3** While holding the install and remove latches, use a continuous, even motion to slide the unit into the slot until the unit engages the midplane. You will feel increased resistance when the unit engages the midplane.



Legend:

1. Top latch
2. Slot
3. Bottom latch

-
- 4** Push evenly on the face of the unit until the unit is flush with the subrack or adjacent units.

If the unit offers excessive resistance to this action, remove the unit and check for bent or broken contacts. If damage is found, do not use that unit. If no damage is found, make sure you are inserting the unit in the correct slot, and try again to insert the unit.

-
- 5** Simultaneously close the install and remove latches at the top and bottom of the unit.

END OF STEPS



ARUs, LHUs, and PSPs

Overview

Purpose This section contains information about the ARU, LHU, and PSP.

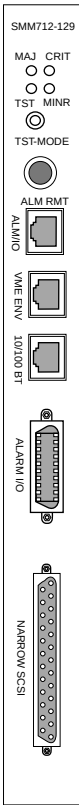
Organisation This section is organised as follows:

- [“About the ARU” \(2-16\)](#)
- [“About the LHU” \(2-18\)](#)
- [“About the PSP” \(2-19\)](#)



About the ARU

Unit description The Alarm Relay Unit (ARU) provides interfaces to system alarm indicators, a network interface to the LHU, and a narrow Small Computer System Interface-2 (SCSI-2) to the MSU. The ARU is located on the back of the Main Controller (MC) subrack. The following illustration shows a front view of the ARU.



Component descriptions The ARU has the following components.

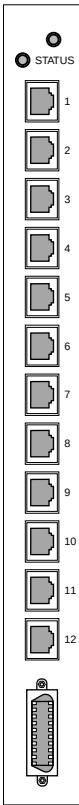
Component	Description
MAJ LED	The Major (MAJ) LED should be ignored. It has no system-related function.
CRIT LED	The Critical (CRIT) LED should be ignored. It has no system-related function.
TST LED	The Test (TST) LED should be ignored. It has no system-related function.
MINR LED	The Minor (MINR) LED should be ignored. It has no system-related function.
TST-MODE switch	Pressing the TST-MODE switch disables alarm signals from the ARU to the ACP.

Component	Description
ALM RMT connector	The ALM RMT connector is a 7-pin mini-DIN connector. The other end of the cable that attaches to this connector attaches to the connector labeled ARU-RELAY 1 on the ACP. This interface carries station alarm signals from the ARU to the ACP.
ALM/IO connector	The ALM/IO connector is an RJ45 female connector. The other end of the cable that attaches to this connector attaches to the connector labeled ARU-ALT 1 on the ACP. For systems with a duplicated MC, the ALM/IO connector on the ARU in the protection MC connects to ARU-ALT 2 on the ACP. This interface carries User Panel alarm signals; for example, system-level Prompt, Deferred, and Information alarm signals, from the ARU to the ACP.
VME ENV connector	The VersaModule Eurocard environment (VME ENV) monitor connector is an RJ45 female connector. The other end of the cable that attaches to this connector attaches to the VME environment monitor connector in the upper right corner of the MC subrack. This interface carries MPU power failure and fan failure alarm signals from the VME environment monitor to the ARU.
10/100 BT connector	The 10/100 BT connector is an RJ45 female connector. The other end of the cable that attaches to this connector attaches to port 1 on the LHU. This interface connects the MC subrack to the MCLAN.
ALARM I/O connector	The ALARM I/O connector is an HD-26 female connector. The other end of the cable that attaches to this connector attaches to the connector labeled ARU-ALARM 1 on the ACP. For systems with a duplicated MC, the ALARM I/O connector on the ARU in the protection MC connects to ARU-ALARM 2 on the ACP. This interface carries Rack Top, End-Of-Suite, and Miscellaneous Discrete alarm signals from the ARU to the ACP.
NARROW SCSI connector	The NARROW SCSI connector is a DB-68 female connector. The other end of the cable that attaches to this connector attaches to the connector labeled SCSI IN on the SCSI TM.



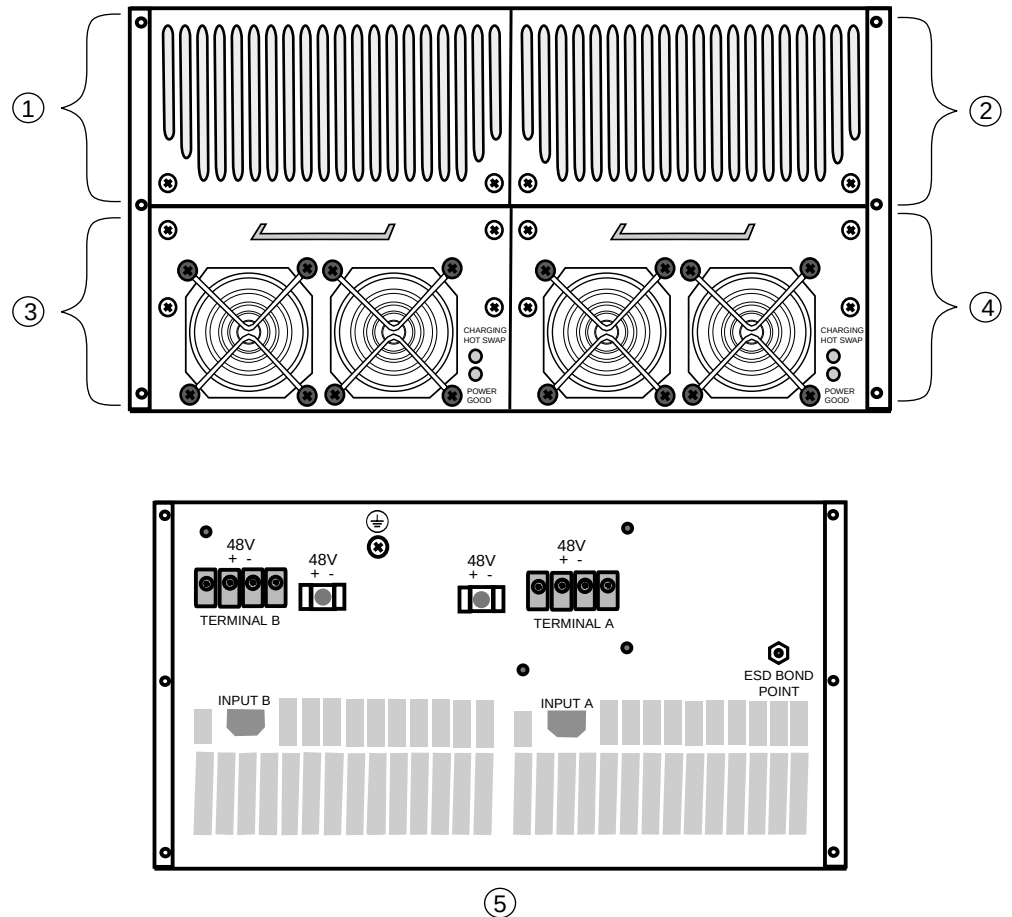
About the LHU

Description The LAN Hub Unit (LHU) provides the hub ports necessary for LAN connections in the system. The system requires at least two LHUs. The LHUs are located on the back of the Main Controller subrack. The following illustration shows the arrangement and numbering of the LHU ports.



About the PSP

Description The Power Supply (PSP) supplies DC power for the midplane, fans, and units in the Main Controller (MC) subrack. The PSP is located below the fan trays at the bottom of the MC subrack. The PSP has its own set of fans that are separate from the fans in the fan trays. Each PSP receives DC power from two sets of terminal blocks, which are located on the back of the MC subrack.



Legend:

1. First fan tray
2. Second fan tray (for duplicated MC configuration)
3. First PSP
4. Second PSP (for duplicated MC configuration)
5. Rear view of PSP



MPUs and MSUs

Overview

Purpose This section contains information about MPU and MSU units.

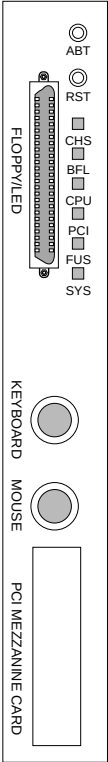
Organisation This section is organised as follows:

- “About the MPU” (2-21)
- “About the MSU” (2-23)



About the MPU

Unit description The Main Processor Unit (MPU) provides the central processing function which includes control of the ARU, LHU, and MSU. The MPU is located on the front of the Main Controller subrack. The following illustration shows a front view of the MPU.



Component descriptions The MPU has the following components.

Component	Description
ABT switch	Pressing the Abort (ABT) switch sends an interrupt signal to the processor, which aborts program execution.
RST switch	Pressing the Reset (RST) switch resets all devices on the MPU and initiates a system reboot.
CHS LED	The Checkstop (CHS) LED is a yellow LED that lights when a halt condition is detected.
BFL LED	The Board Failure (BFL) LED is a yellow LED that lights when a board failure condition is detected. If the BFL LED lights, replace the MPU.
CPU LED	The CPU activity (CPU) LED is a green LED that lights when the processor bus is active.

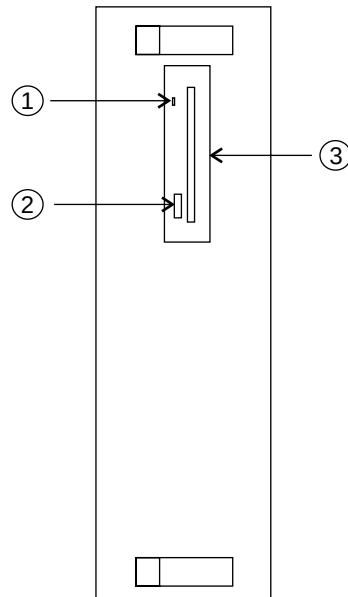
Component	Description
PCI LED	The PCI activity (PCI) LED is a green LED that lights when the PCI bus is active. This LED lights only if a PCI mezzanine card is installed. A PCI mezzanine card is not supported in this release.
FUS LED	The Fuse OK (FUS) LED is a green LED that lights when all fuses are intact and power is available from the MPU to the transition modules and other devices in the Main Controller subrack. If the FUS LED is <i>not</i> lit, replace the MPU.
SYS LED	The System Controller (SYS) LED is a green LED that lights when the MPU is the system controller.
FLOPPY/LED connector	The FLOPPY/LED connector should not be used in this release. Do not attach any equipment to this connector.
KEYBOARD connector	The KEYBOARD connector should not be used in this release. Do not attach any equipment to this connector.
MOUSE connector	The MOUSE connector should not be used in this release. Do not attach any equipment to this connector.
PCI MEZZANINE CARD	The slot for a PCI mezzanine card should not be used in this release.

Related topic For more information, see “Clearing a FLTcEQ on an MPU” (21-69).



About the MSU

Description The Mass Storage Unit (MSU) contains a hard disk drive and a Magneto-Optical (MO) drive. The MSU is located on the front of the Main Controller subrack. The following illustration shows a front view of the MSU.



Legend:

1. Activity indicator
2. Release button
3. MO disk drive

Related topic For more information, see “Clearing a FLTcEQ on an MSU” (21-70). □

Serial TM, NIC TM, and SCSI TM

Overview

Purpose This section contains information about Serial Transition Module (TM), Network Interface Chip (NIC) TM, and Small Computer System Interface (SCSI) TM units. These units are all located on the back of the Main Controller subrack.

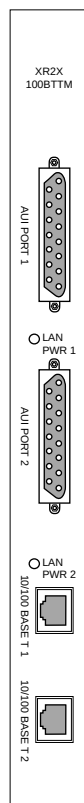
Organisation This section is organised as follows:

- [“About the NIC TM” \(2-25\)](#)
- [“About the SCSI TM” \(2-27\)](#)
- [“About the Serial TM” \(2-28\)](#)



About the NIC TM

Unit description The Network Interface Chip (NIC) Transition Module (TM) provides LAN access to the MPU. The NIC TM is located on the back of the Main Controller subrack. The following illustration shows a front view of the NIC TM.



Component descriptions The NIC TM has the following components.

Component	Description
AUI PORT 1 connector	The AUI PORT 1 connector is not used in this release.
LAN PWR 1 LED	The LAN PWR 1 LED lights when power is on for the MC subrack.
AUI PORT 2 connector	The AUI PORT 2 connector is not used in this release.
LAN PWR 2 LED	The LAN PWR 2 LED lights when power is on for the MC subrack.
10/100 BASE T 1 connector	The 10/100 BASE T 1 connector is not used in this release.

Component	Description
10/100 BASE T 2 connector	The 10/100 BASE T 2 connector is an RJ45 female connector. This connector is used to connect the DACS system to a customer-premises LAN.



About the SCSI TM

Unit description The Small Computer System Interface (SCSI) Transition Module (TM) provides a narrow SCSI-2 interface between the MPU and the MSU. The SCSI TM is located on the back of the Main Controller subrack. The following illustration shows a front view of the SCSI TM.



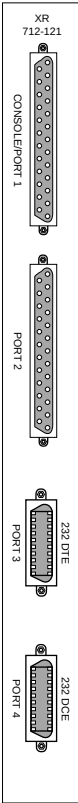
Component descriptions The SCSI TM has the following components.

Component	Description
SCSI IN connector	The SCSI IN connector is a DB-68 female connector. The other end of the cable that attaches to this connector attaches to the connector labeled NARROW SCSI on the ARU.
SCSI OUT connector	The SCSI OUT connector is a DB-68 female connector. An active SCSI bus terminator attaches to this connector. <i>The MSU will not operate properly if the SCSI bus terminator is removed.</i>



About the Serial TM

Unit description The Serial Transition Module (TM) provides serial I/O access to the MPU. The Serial TM is located on the back of the Main Controller subrack. The following illustration shows a front view of the Serial TM.



Component descriptions The Serial TM has the following components.

Component	Description
CONSOLE/ PORT 1 connector	The CONSOLE/PORT 1 connector is a DB-25 female connector. This connector provides a 9600 bps, V.28 DCE interface to the MPU. A VT100-compliant terminal can be connected to CONSOLE/PORT 1 for use as a system console.
PORT 2 connector	The PORT 2 connector is a DB-25 female connector. This connector provides a 16550-compatible, V.28 DTE interface to the MPU. PORT 2 can be used for serial Point-to-Point-Protocol access to the system from a Wide Area Network.

Component	Description
PORT 3 connector	The PORT 3 connector is an HD-26 female connector. This connector provides a 115.2 Kbps asynchronous V.28 DTE interface to the MPU for serial Point-to-Point-Protocol access to the system. PORT 3 can be used to connect to a Network Management System.
PORT 4 connector	The PORT 4 connector is an HD-26 female connector. The other end of the cable that attaches to this connector is a daisy-chain cable that attaches to the LHUs, and provides a dedicated interface for control and management of the LHUs.



Unit codes and spare equipment list

Overview

Purpose This section contains information about unit codes, and the recommended list of spare equipment.

Organisation This section is organised as follows:

- “Unit codes” (2-31)
- “Recommended spare equipment” (2-32)



Unit codes

Downward compatible units

Units with more than one version have a lettered suffix after the unit code. For example: the LAH101 and the LAH101B are different versions of the same unit. The LAH101B is a later software version of the LAH101. The unit with the later version will work just as well as the earlier version in the same slot, but some new features will not work until you upgrade the software.

Downward compatible units are sometimes referred to as backward compatible.

New codes

A unit is *not* downward compatible when it has a new code. A new unit code usually means that the new unit requires a different software configuration.



Recommended spare equipment

List of recommended spares

The following is a list of recommended spare equipment.

Equipment	Quantity
700W DC power supply for MC subrack	1
ARU	1
BSC	1
DTU	1
Dual fan tray for MC subrack	1
Fan filter for MC subrack	2
MPU	1
MSU	1
NIC-TM	1
PTM	1
Serial-TM	1
SCSI-TM	1
SCSI-Term	1
SRC	1
STU	1





3 About cables

Overview

Purpose “About cables” describes the system fibre-optic cables, cable connections, and how to insert and remove fibre-optic cables.

Organisation “About cables” is organised as follows:

- “About cables” (3-2)
- “Inserting a cable” (3-3)
- “Removing a cable” (3-4)
- “About internal fibre connections” (3-5)

Related topic For information about cable connections, see the *Installation Assembly Manual*.



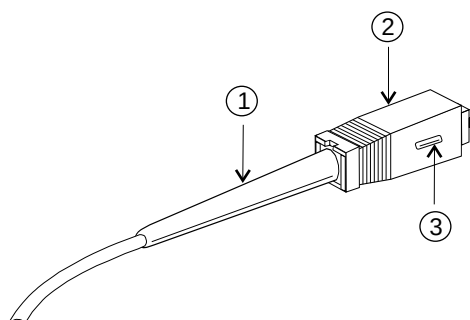
About cables

Important! Cables are also referred to as fibre-optic cables.

SC fibre-optic cables The following units have SC cables attached to them:

- OLU
- BSSUs
- BSIUs on the PSA subrack
- STM-1s with IM01 or IM04 Interface Units

The following illustration shows an example of an SC cable.



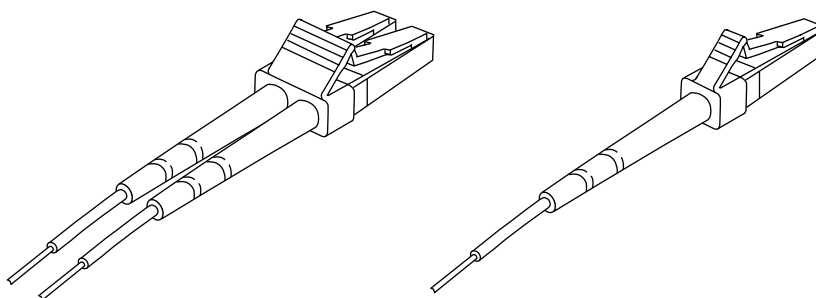
Legend:

1. Boot
2. Sleeve
3. Key

LC fibre-optic cables The following units have LC cables attached to them:

- STM-4s
- STM-16s
- BSIUs on the PSC subrack
- STM-1s with IM09 Interface Units

The following illustration shows an example of two types of LC cables.



Inserting a cable

Procedure

- 1 Align the cable with the cable connector.

Some cables and cable connectors are keyed. Align the key on the optical connector with the slot on the cable connector before you insert the cable into the connector.

Reference:

For a diagram, see “About cables” (3-2).

- 2 While holding on to the cable sleeve, insert the cable into the cable connector.
-

- 3 While holding on to the cable boot, give the cable an extra push to make sure the cable is firmly engaged and locked in place. You should hear a click when the cable locks into the connector.

If a cable is not secure, slight movements of the cable can cause transmission errors.

END OF STEPS



Removing a cable

Procedure

- 1 If you plan to reattach the cables, label the cables so that you know where to reattach them.
-

- 2 Grasp the sleeve on the end of the cable.

Reference:

For a diagram, see “About cables” (3-2).

Important! Do not pull on the boot or fiber to disconnect a cable.

- 3 Pull on the sleeve to release the cable.
-

- 4 Remove the cable.

END OF STEPS



About internal fibre connections

- BSFI interfaces** The Bit Slice Fibre Interface (BSFI) is the timing and control link between the BSC and BSSUs. Fibre-optic cables provide this interface. The actual link occurs between the BSSUs and the OLU's located on the back of the Matrix and Synchronisation subrack.
- ECI interfaces** The Equipment Core Interface (ECI) is a 622 Mbps transmission interface between the BSIUs in the port subracks and the BSSUs in the Matrix and Control subrack and the Matrix and Synchronisation subrack. Fibre-optic cables with SC or LC connectors provide this interface.
- Related topics** For the latest diagrams of the BSFI and ECI interfaces, see the *Installation Assembly Manual*. Lucent personnel can view the assembly manual at <http://www2.mv.lucent.com/wsdacs/wsdacs/Default.htm>. If you do not have access to this website, ask your account representative or technical support for the latest diagrams.





4 About the user interface

Overview

Purpose “About the user interface” describes the user interface. The user interface is used to perform operations, administration, maintenance, and provisioning tasks on the Digital Access and Cross-connect System (DACS).

What you need to know A basic knowledge of *Microsoft Windows NT*[®] is assumed.

Getting started To log on to the network element (DACS), you will need a valid user ID and password for both the PC and the DACS.

Organisation “About the user interface” is organised as follows:

- [“About the user-interface PC” \(4-2\)](#)
- [“Logging on” \(4-4\)](#)
- [“Logging off” \(4-6\)](#)
- [“Structure of the user interface” \(4-8\)](#)
- [“About the main application window” \(4-10\)](#)
- [“About query results windows” \(4-14\)](#)
- [“Updating data from a query results window” \(4-16\)](#)
- [“Button descriptions” \(4-17\)](#)
- [“Key descriptions” \(4-20\)](#)
- [“About system messages” \(4-22\)](#)
- [“About Help” \(4-23\)](#)

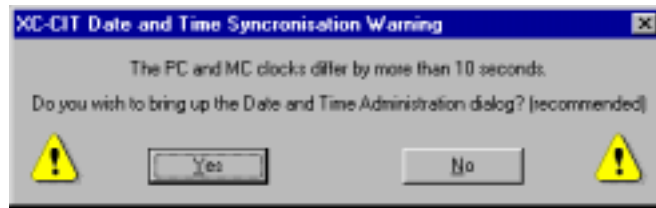


About the user-interface PC

General information about the PC	A Personal Computer (PC) running the user interface application software is required to perform operations, administration, maintenance, or provisioning tasks on the system. The PC is also called a Craft Interface Terminal (CIT). The user interface application software, called XC-CIT, provides a point-and-click graphical user interface. You point and click to select values or options, then point and click to apply them. XC-CIT works best when the PC does <i>not</i> have other software installed.
Booting the PC	You can boot the PC with or without a link to the system. If you boot a PC with an active link to the system, it will not affect service. However, booting will cause the link to the system to be dropped. You must log back on to the system to reestablish the link.
Number of user interface sessions	Up to six user interface sessions can be connected to one DACS system at the same time. All six user interface sessions can be running on one PC, or there can be up to six local and/or remote PCs.
Other users logging on to the system	PCs already logged on to the system will not be affected by a new user logging on to the system.
About connecting a PC to more than one DACS	If the PCs are on a LAN that has more than one DACS, each PC can connect to more than one DACS. To connect to more than one DACS, a PC must have XC-CIT application software for each DACS.
Link failure message	The system displays a failure message if the link between a PC and a DACS fails. You must log back on to the system to reestablish the link.
Socket failure message	The system displays a failure message if a communication error is detected. If the socket failure message displays, check the TCP/IP connection and parameters.

**Date and time
synchronisation warning**

The system displays the following warning if the PC date and time is more than 10 seconds different from the system (Main Controller) date and time.



If you click Yes, the Date and Time Administration window appears, and you can change the PC date and time or the system date and time.

If you click No, the warning window closes, and the PC and system date and time remain unchanged.



Logging on

Login window



Field descriptions The Login window has the following fields.

Field	Description
Login ID	The Login ID is a unique user login identification that must have from two to eight letters or numbers. The first character must be a letter, and at least one character must be a lowercase letter. A default login ID is provided for the system administrator. Only the system administrator can add or remove a login ID.
Password	The password must have from four to eight characters. There are no restrictions on what characters you can use in the password.
Network Element	The Network Element field must contain a network element name or an IP address. • If a network element name has been provisioned, use the name of the network element. • If a network element name has not been provisioned, use the IP address.

Procedure

- 1 Enter your login ID.
- 2 Enter your password.
- 3 Enter the appropriate network element.

4 Click Connect.

END OF STEPS



Logging off

Log off the system

There are two ways to log off the system:

- Click the X in the upper right-hand corner of the user-interface window.
- Go to *File > Exit*.

The system will display a confirmation window.

Respond to the confirmation by clicking the appropriate button.



Displaying the name of the system that the PC is connected to

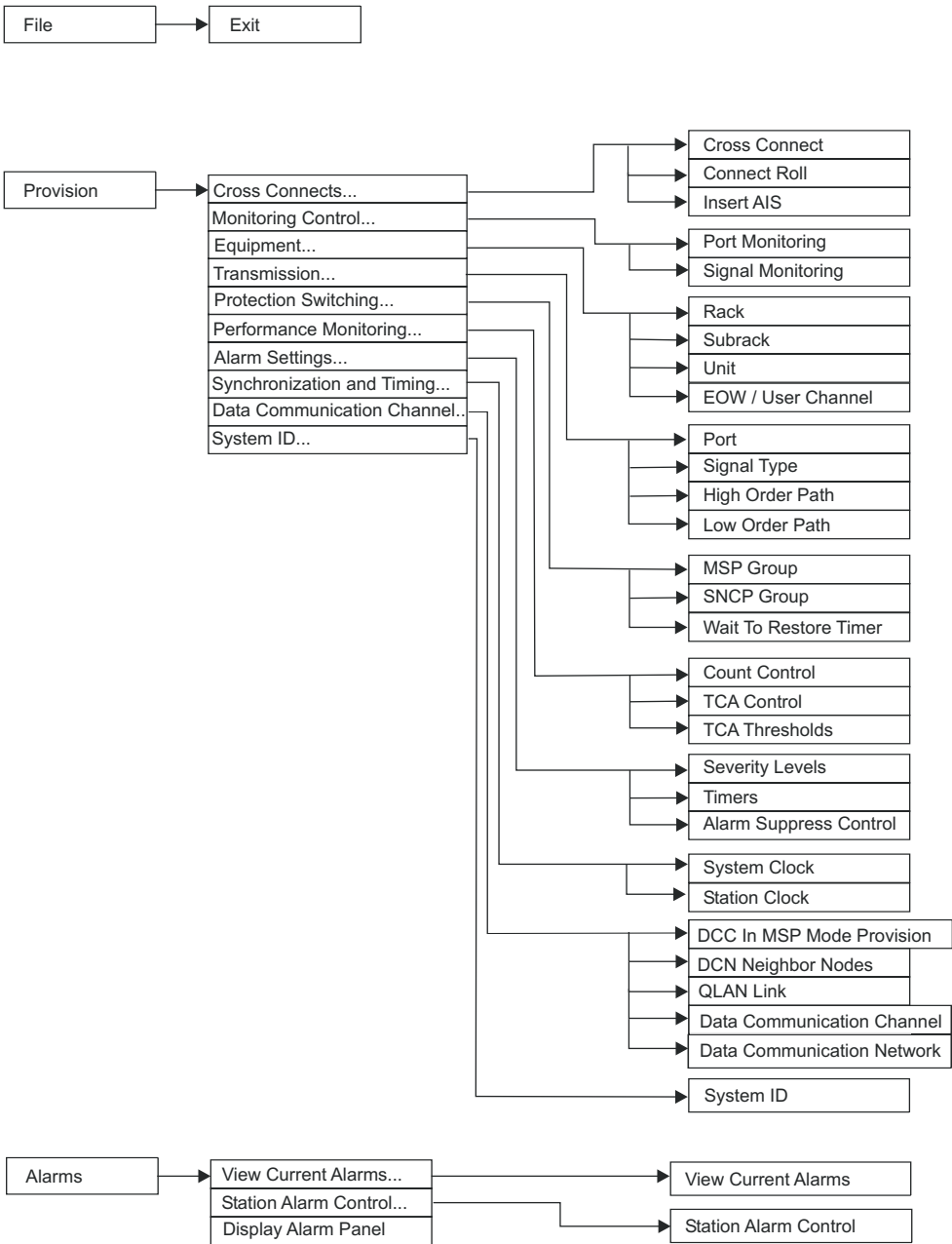
Display PC connected to name

To display the name of the system that the PC is connected to, go to
Help > About....



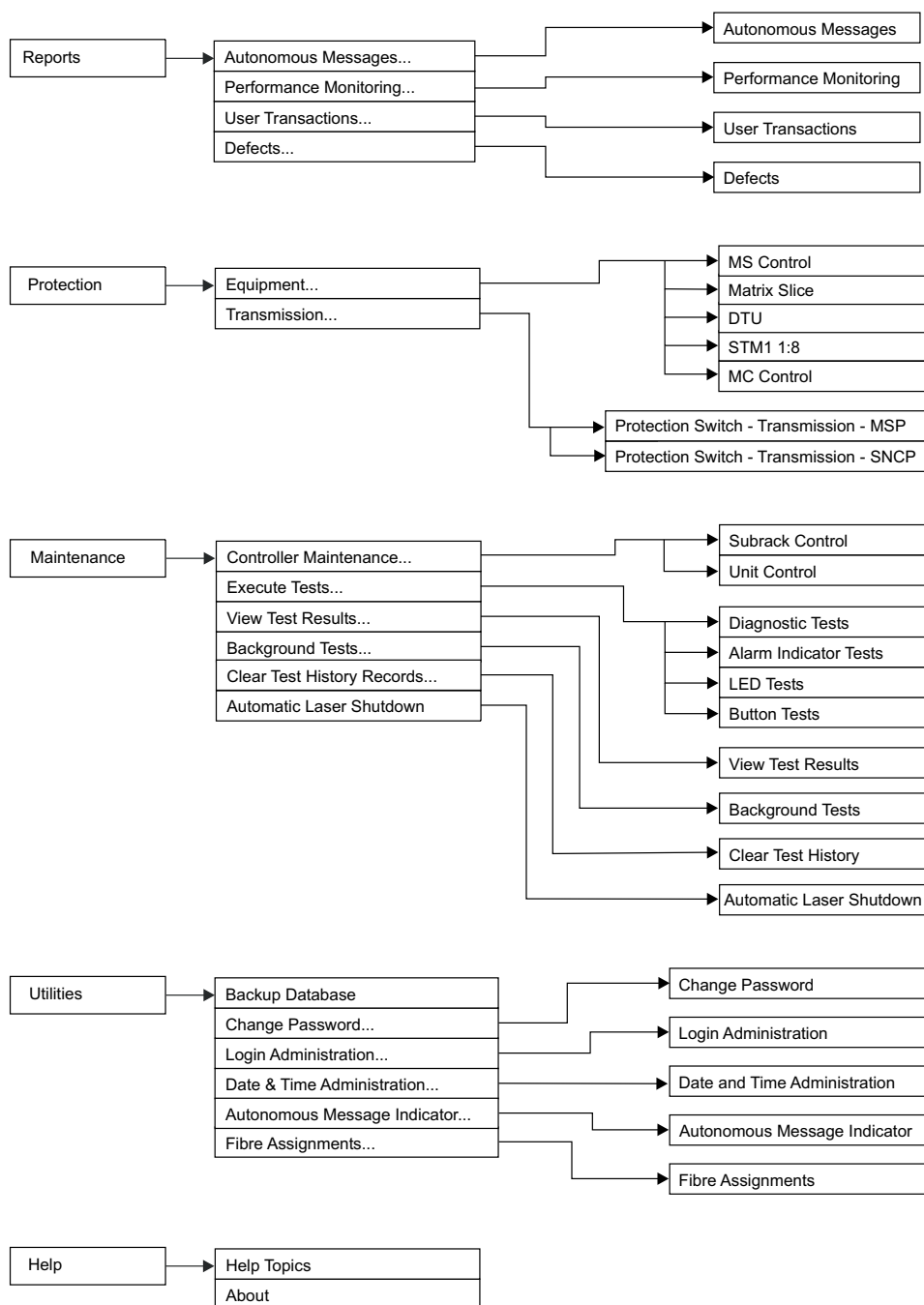
Structure of the user interface

File, Provision, and Alarms menus The following graphic shows the arrangement of the File, Provision, and Alarms menus.



Reports, Protection, Maintenance, Utilities, and Help menus

The following graphic shows the arrangement of the Reports, Protection, Maintenance, Utilities, and Help menus.



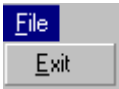
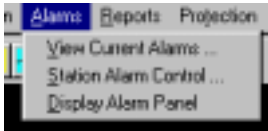
About the main application window

Description The main application window contains a title bar, a menu bar, and a toolbar.

Menu bar



The menu bar contains the menus that open the windows that you use for provisioning and maintaining the system. The menu bar appears at the top of the application window directly below the title bar.

Item	Function
File	The File menu provides access to the Exit function. 
Provision	The Provision menu provides access to the parts of the system that require provisioning. 
Alarms	The Alarms menu provides access to the windows from which you can perform alarm-related tasks other than alarm provisioning. 

Item	Function
Reports	The Reports menu provides access to the windows from which you can display or print various reports. The following reports are located elsewhere in the user interface: - To display and print current alarms, go to <i>Alarms</i> > <i>View Current Alarms</i>. - To display and print diagnostic test results, go to <i>Maintenance</i> > <i>View Test Results</i>.
Protection	The Protection menu provides access to the windows from which you can perform protection switch requests and display protection switch-related information. To provision protection switching groups and Wait-To-Restore timers, go to <i>Provision</i> > <i>Protection Switching</i>.
Maintenance	The Maintenance menu provides access to the windows from which you can perform maintenance-related tasks.
Utilities	The Utilities menu provides access to the windows from which you can perform general system-related tasks.

Item	Function
Help	The Help menu provides access to Help Topics and the About... window. 

Toolbar



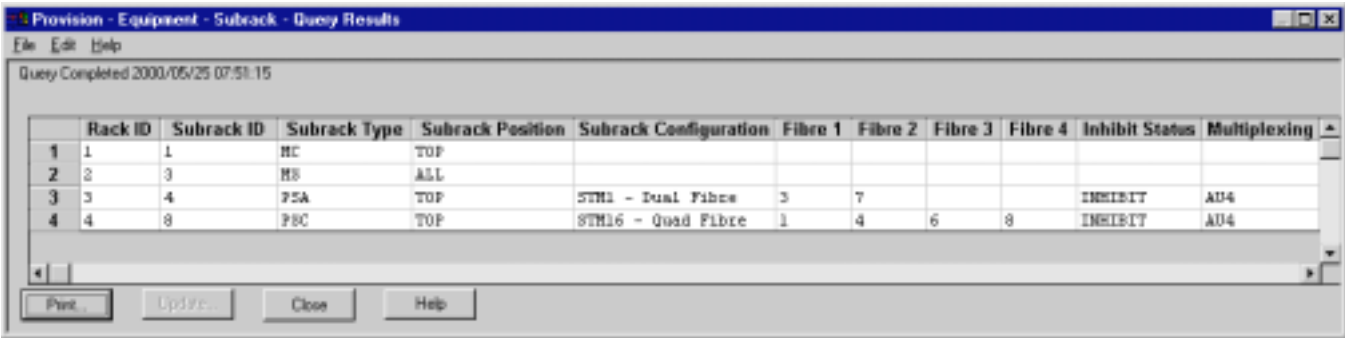
The toolbar is located directly beneath the menu bar. It provides quick access to frequently-used windows.

Button	Function
Cross-connect provisioning button 	The Cross-connect provisioning button opens to the Cross Connect window.
Monitoring control provisioning button 	The Monitoring control provisioning button opens to the Port Monitoring window.
Equipment provisioning button 	The Equipment provisioning button opens to the Rack window.
Transmission provisioning button 	The Transmission provisioning button opens to the Port window.
Performance monitoring provisioning button 	The Performance monitoring provisioning button opens to the Count Control window.
View current alarms button 	The View current alarms button opens to the View Current Alarms window.
Autonomous messages report button 	The Autonomous messages report button opens to the Reports — Autonomous Messages window.

Button	Function
Performance monitoring report button 	The Performance monitoring report button opens to the Reports — Performance Monitoring window.

About query results windows

Illustration Use the following illustration only as an example of a query results window.



Important! The data displayed on this screen may *not* be typical.

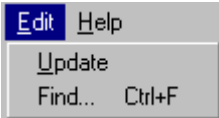
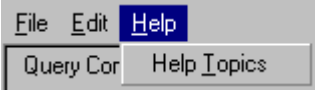
Sorting query records Double-clicking on a column heading in a query results window sorts the information in that column either numerically or alphabetically.

Query results menu bar



The query results menu bar is displayed across the top of the query results window.

Item	Function
File	The File menu provides access to the menu list items for saving to a file and printing. FileEditHelp Save As... Print...Ctrl+P Print Preview Page Setup... Print Setup... Exit

Item	Function
Edit	The Edit menu provides access to the menu list items Update and Find. • Use Update to replace the data in the window from which the query was performed with data from a record that you select from the query results window. This is useful when you want to change the query results data without having to enter the information in the original window. For more information, see “Updating data from a query results window” (4-16). • Use Find to locate a specific record in the query results. 
Help	The Help menu provides access to help for query results windows. 



Updating data from a query results window

Procedure Do the following when you want to change the query results data without having to enter the information in the original query results window.

1 Perform a query.

2 Do any of the following:

- Highlight a record and press the update button at the bottom of the window.
- Highlight a record and select Update from *Edit > Update*.
- Double-click on the record.

END OF STEPS



Button descriptions

Button descriptions The following section describes the buttons that may appear at the bottom of the user interface windows.

Button	Function
Apply	The Apply button changes or creates a database record.
Autonomous Events	The Autonomous Events button opens the Autonomous Messages window.
Cancel Test	The Cancel Test button cancels the selected background test.
Change	The Change button changes a database record.
Clear	The Clear button clears the fields and restores the window to its original state.
Clear AIS	The Clear AIS button removes AIS (Alarm Indication Signal) on an entity.
Clear Records	The Clear Records button clears the records for the specified tests.
Close	The Close button closes the window.
Connect	The Connect button on the Cross Connect window creates a cross connect. The Connect button on the Login window establishes a connection to a local or remote network element.
Connect Station Alarms	The Connect Station Alarms button connects the station alarm indicators so that they will light or sound when a station alarm is active.
Create	The Create button creates a record in the database.
Current Alarms	The Current Alarms button opens the View Current Alarms window.
Delete	The Delete button deletes one or more database records.
Disconnect	The Disconnect button removes a cross connect.
Disconnect Station Alarms	The Disconnect Station Alarms button disconnects station alarm indicators. Pressing the Disconnect Station Alarms button will not affect LED indicators on units and station alarm indicators that cannot be disconnected.
Execute	The Execute button initiates a test.

Button	Function
Help	The Help button opens a screen-related help topic window.
Initialise	The Initialise button initialises a unit controller.
Insert AIS	The Insert AIS button inserts AIS (Alarm Indication Signal) on an entity.
Manual Restart	The Manual Restart button restarts a laser that the system has previously shutdown by performing a 2-second transmission test. If there are no problems, the signal is restored.
Manual Restart for Test	The Manual Restart for Test button restarts a laser that the system has previously shutdown by performing a 90-second transmission test. If there are no problems, the signal is restored.
Monitoring Control...	The Monitoring Control... button opens the Monitoring Control window.
Print	The Print button opens the <i>Microsoft Windows NT[®]</i> print dialog box.
Protection Switch Control	The Protection Switch Control button opens the Matrix Control window.
Query	The Query button requests information from the system database.
Query Active	The Query Active button queries the active STU.
Query From ID	The Query From ID button queries the From ID address for the source of the cross-connect data.
Query NE Date/Time	The Query NE Date/Time button queries the network element date and time, and uses it to overwrite the Date and Time fields on the Date and Time Administration window.
Query PC Date/Time	The Query PC Date/Time button queries the personal computer date and time, and uses it to overwrite the Date and Time fields on the Date and Time Administration window.
Query Port	From the Automatic Laser Shutdown window, the Query Port button opens the Port window, which can be used to enable or disable the automatic laser shutdown feature.
Query Standby	The Query Standby button queries the standby STU.
Query To ID	The Query To ID button queries the To ID address for the destination of the cross-connect data.

Button	Function
Remove	The Remove button removes an MPU or SRC from service.
Restore	The Restore button restores an SRC to service.
Restore All	The Restore All button restores all alarm severities to their default values.
Roll	The Roll button rolls a cross connect.
Save Error Message	The Save Error Message button saves the error message to a common file on the PC.
Set NE Date/Time	The Set NE Date/Time button changes the date and time for the network element to the values displayed in the Date and Time fields on the Date and Time Administration window.
Set PC Date/Time	The Set PC Date/Time button changes the date and time on the PC to the values displayed in the Date and Time fields on the Date and Time Administration window.
Subrack Degrade Inhibit	The Subrack Degrade Inhibit button opens the Subrack window, which can be used to enable or disable the Degrade Inhibit feature.
Suppress Station Alarms	The Suppress Station Alarms button causes a system-wide temporary suppression of current station alarm indicators. Pressing the Suppress Station Alarms button will not affect LED indicators on units and station alarm indicators that cannot be suppressed, nor will it affect indicators for future alarms.
Update	The Update button replaces the data in the window from which the query was performed with data from a record that you select from the query results window.
View Results	The View Results button displays the requested test results.
WTR Timer	The WTR Timer button opens the Wait To Restore Timer window.



Key descriptions

Keys used for shortcuts Shortcut keys are combinations of keys that you press to perform an action that you would otherwise perform with the mouse. As in other *Microsoft Windows NT*® applications, shortcut keys are a combination of the ALT key and the underlined letter associated with a menu or menu item.

Example

Pressing **ALT + P** opens the Provision menu.



Keys used for editing For windows that permit data entry, an Edit menu with cut, copy, and paste functions is available. You can also perform these editing functions by using the following keys.

Key	Function
CTRL+X	Removes the selected information
CTRL+C	Copies the selected information
CTRL+V	Pastes the cut or copied information into the selected input field

Keys used for navigation Navigation in the user interface is accomplished primarily by clicking, double-clicking, and scrolling with a mouse. You can also use the following keys for navigation.

Key	Moves the cursor
Left arrow	Left one field or subfield
Right arrow	Right one field or subfield
Up arrow	Up one item in a drop list or field
Down arrow	Down one item in a drop list or field
Home	To the beginning of items in a drop list

Key	Moves the cursor
End	To the end of items in a drop list
Page Up	Up one screen
Page Down	Down one screen
Tab	To the next field or command button
Shift Tab	To the previous field or command button

About system messages

General system messages A message window may appear when you are performing provisioning and maintenance tasks. You can get help for a system message by clicking the Help button on the system message window. The help associated with a system message explains why this message has occurred and suggests corrective actions.

Time-out message The system displays a time-out message if your request cannot be processed in a reasonable amount of time. If you get a time-out message, wait a few minutes, then try the request again.



About Help

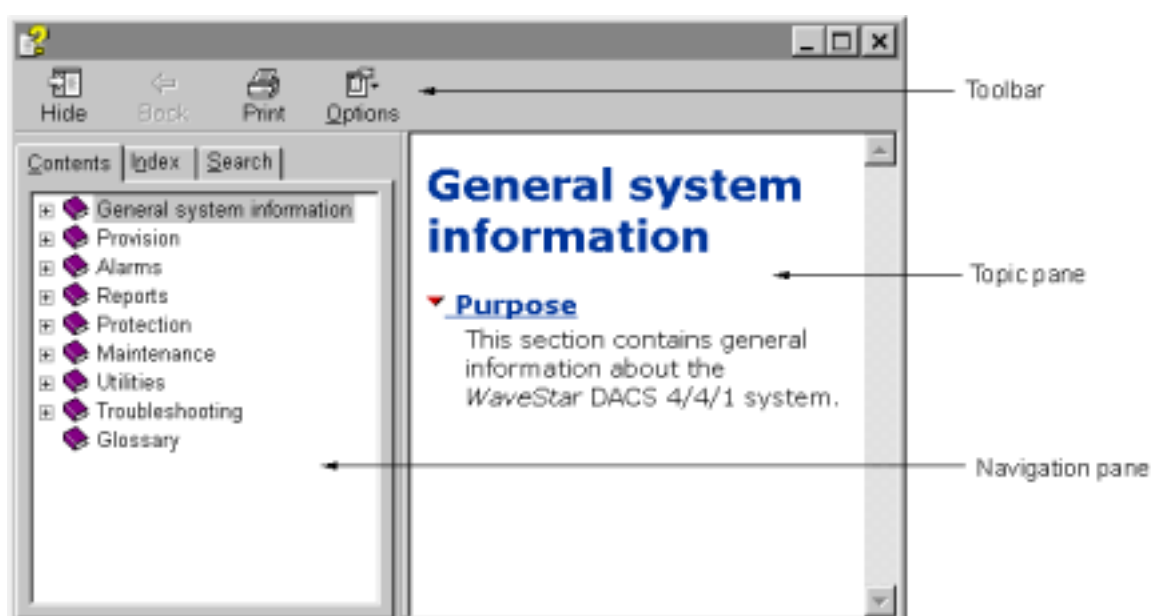
Help Topics Selecting Help Topics from the Help menu opens the help system. The help system and the paper documentation are almost identical because they are derived from the same source. The help system works best if you have *Microsoft Internet Explorer*® 4.0 or later installed on your PC.

About... Selecting About... from the Help menu opens a window that contains information about the current software version and the maximum system capacity.

Accessing Help There are two ways to access the help system:

- Click on the Help button from any user interface window to display a help topic that is specific to that window.
- Go to *Help > Help Topics*.

The Help Topics window The following illustration shows the Help Topics window.



The Help Topics window has a toolbar, navigation pane, and topic pane.

The Help toolbar The Help toolbar has the following buttons.

Button	Function
Hide	If the navigation pane is open, clicking the Hide button closes the pane. If the navigation pane is closed, clicking the Hide button opens the pane.
Back	Clicking the Back button opens the previously viewed help topic in the topic pane.
Print	Clicking the Print button opens a dialog box from which you choose whether to print the selected topic (the topic currently displayed in the topic panel), or if a heading is selected in the navigation pane, the selected heading and all subtopics.
Options	Clicking the Options button opens a menu that contains the following items: • Hide Tabs — performs the same function as the Hide button. • Back — performs the same function as the Back button. • Stop — stops a web page from opening. This help system does not have links to internet web pages. • Refresh — refreshes the topic that appears in the topic pane. • Internet Options — opens a dialog box from which you can set various options for <i>Internet Explorer</i>. • Print — performs the same function as the Print button. • Search Highlight On/Off— turns on or off the Search Highlight function. The Search Highlight function highlights the word or words that you search for using the Search tab.

The navigation pane

The navigation pane has the following tabs that help you find the appropriate help topic.

Tab	Function
Contents	The Contents tab displays an expandable list of help topics. Items in the list that can be expanded have a book icon and a plus sign to the left of the item. To expand an item, click on the plus sign, or double-click on the item. To select a help topic, click on an item in the list. The selected help topic appears in the topic pane.
Index	The Index tab displays a list of index entries. To select a help topic, click on an item in the list, or type a word into the text box above the list and press ENTER when the desired index entry is highlighted. The selected help topic appears in the topic pane.
Search	The Search tab lets you search for one or more words that appear in the help topics. To search for a word, type the word to search for and press ENTER . A list of help topics that contain the search word appears. To select a help topic, double-click on an item in the list. The selected help topic appears in the topic pane.

The topic pane The topic pane displays the selected help topic.





5 About equipment and signal addresses

Overview

Purpose “About equipment and signal addresses” contains general information about equipment and signal addresses that appear on the user interface.

Organisation “About equipment and signal addresses” is organised as follows:

- “About entity addresses” (5-2)
- “About physical layer addresses” (5-3)
- “About signal layer addresses” (5-4)
- “Wildcard addresses” (5-9)
- “256 and 512 addressing” (5-10)
- “MC entity addresses” (5-11)
- “MS entity addresses” (5-12)
- “PSA entity addresses” (5-13)
- “PSC entity addresses” (5-14)
- “Equipment protection group addresses” (5-16)
- “MSP addresses” (5-17)
- “RT addresses” (5-18)
- “Fibre addresses” (5-19)



About entity addresses

Description of physical and signal layers

The entity address consists of two parts: a physical layer and a signal layer. In the following example, the physical layer is labelled Port ID, and the signal layer is labelled Signal ID.

The screenshot shows a configuration window with two main sections. The top section is for 'Port ID' and contains five dropdown menus labeled 'Subrack', 'Number', 'Unit', 'Number', and 'Port'. The values are 'PSA', '4', 'STM1', '1', and '1' respectively. The bottom section is for 'Signal ID' and contains a dropdown menu labeled 'Select' with the value 'AUG#1 - AU4 - ALL'.

Subrack	Number	Unit	Number	Port
PSA	4	STM1	1	1

Signal ID: Select AUG#1 - AU4 - ALL



About physical layer addresses

About the physical layer

The physical layer is part of the entity address; it describes the physical location of the equipment. On most user-interface windows, the physical layer is labelled Port ID, but depending on the context of the window, this field can also be labelled Subrack ID, Unit ID, MSP ID, MSP Group ID, or Protection Group ID.

The physical layer consists of up to five fields:

- subrack
- (subrack) number
- unit
- (unit) number
- port



About signal layer addresses

About the signal layer The signal layer is part of the entity address; it describes the structure of a Synchronous Digital Hierarchy (SDH) signal. The signal layer is always labelled Signal ID on the user interface.

The signal layer consists of the following fields:

- AUG4 number
- AUG1 number
- AU type
- TUG3 value
- TUG2 value
- TU12 value

Table of signal layer addresses The following table shows the valid signal type and entity ID combinations for specifying multiplexing.

Signal Type	Entity ID
AU-4-4c	PSC-s-STM16-u-p-ALL ¹
	PSC-s-STM16-u-p-AUG4#{1-4}-AU4_4c
	PSC-s-STM4-u-p-AUG4#1-AU4_4c
AU-4	PSA-s-STM1-u-p-AUG1#1-AU4
	PSC-s-STM16-u-p-ALL
	PSC-s-STM16-u-p-AUG4#{1-4}-ALL
	PSC-s-STM16-u-p-AUG4#{1-4}-AUG1#{1-4}-AU4
	PSC-s-STM4-u-p-AUG4#1-ALL
	PSC-s-STM4-u-p-AUG4#1-AUG1#{1-4}-ALL
	PSC-s-STM4-u-p-AUG4#1-AUG1#{1-4}-AU4
AU-3	PSA-s-STM1-u-p-AUG1#1-ALL
	PSC-s-STM16-u-p-ALL
	PSC-s-STM16-u-p-AUG4#{1-4}-ALL
	PSC-s-STM16-u-p-AUG4#{1-4}-AUG1#{1-4}-ALL
	PSC-s-STM4-u-p-AUG4#1-ALL
	PSC-s-STM4-u-p-AUG4#1-AUG1#{1-4}-ALL

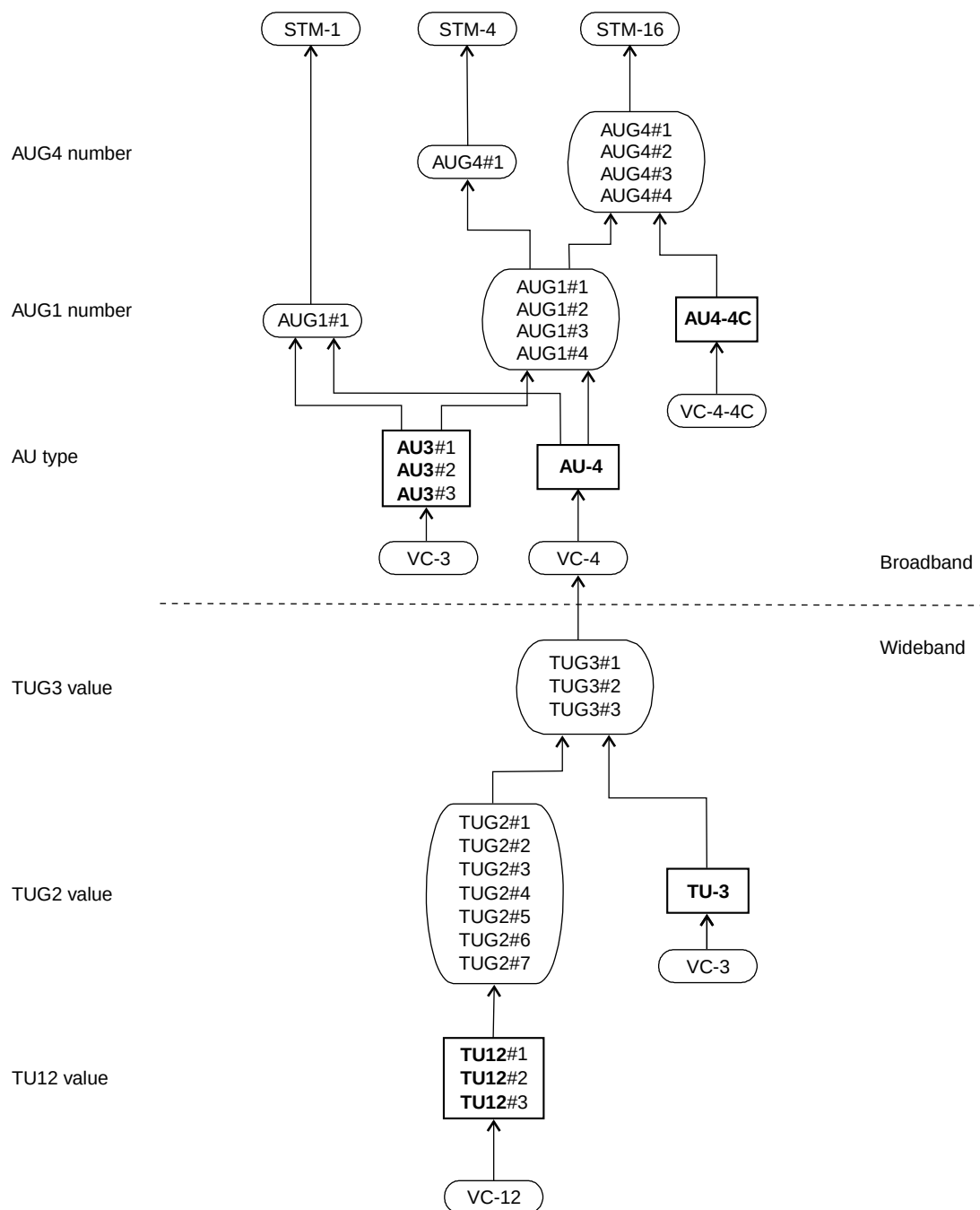
Signal Type	Entity ID
TU-3	PSA-s-STM1-u-p-AUG1#1-AU4-ALL[-ALL] ²
	PSA-s-STM1-u-p-AUG1#1-ALL-TUG3#{1-3}-ALL ³
	PSA-s-STM1-u-p-AUG1#1-ALL-TUG3#{1-3}-TU3 ³
	PSC-s-STM16-u-p-ALL
	PSC-s-STM16-u-p-AUG4#{1-4}-ALL[-ALL]
	PSC-s-STM16-u-p-AUG4#{1-4}-AUG1#{1-4}-ALL
	PSC-s-STM16-u-p-AUG4#{1-4}-AUG1#{1-4}-AU4-ALL
	PSC-s-STM16-u-p-AUG4#{1-4}-AUG1#{1-4}-AU4-TUG3#{1-3}-ALL ³
	PSC-s-STM16-u-p-AUG4#{1-4}-AUG1#{1-4}-AU4-TUG3#{1-3}-TU3 ³
	PSC-s-STM4-u-p-AUG4#1-ALL
	PSC-s-STM4-u-p-AUG4#1-AUG1#{1-4}-ALL
	PSC-s-STM4-u-p-AUG4#1-AUG1#{1-4}-AU4
	PSC-s-STM4-u-p-AUG4#1-AUG1#{1-4}-AU4-TUG3#{1-3}-ALL ³
	PSC-s-STM4-u-p-AUG4#1-AUG1#{1-4}-AU4-TUG3#{1-3}-TU3 ³

Signal Type	Entity ID
TU-12	PSA-s-STM1-u-p-AUG1#1-AU4-ALL[-ALL][-ALL] ²
	PSA-s-STM1-u-p-AUG1#1-AU4-TUG3#{1-3}-ALL[-ALL] ³
	PSC-s-STM16-u-p-ALL
	PSC-s-STM16-u-p-AUG4#{1-4}-ALL[-ALL]
	PSC-s-STM16-u-p-AUG4#{1-4}-AUG1#{1-4}-ALL
	PSC-s-STM16-u-p-AUG4#{1-4}-AUG1#{1-4}-AU4-ALL
	PSC-s-STM16-u-p-AUG4#{1-4}-AUG1#{1-4}-AU4-TUG3#{1-3}-ALL ³
	PSC-s-STM16-u-p-AUG4#{1-4}-AUG1#{1-4}-AU4-TUG3#{1-3}-ALL[-ALL] ³
	PSC-s-STM4-u-p-AUG4#1-ALL
	PSC-s-STM4-u-p-AUG4#1-AUG1#{1-4}-ALL
	PSC-s-STM4-u-p-AUG4#1-AUG1#{1-4}-AU4
	PSC-s-STM4-u-p-AUG4#1-AUG1#{1-4}-AU4-TUG3#{1-3}-ALL ³
	PSC-s-STM4-u-p-AUG4#1-AUG1#{1-4}-AU4-TUG3#{1-3}-ALL[-ALL] ³

Notes:

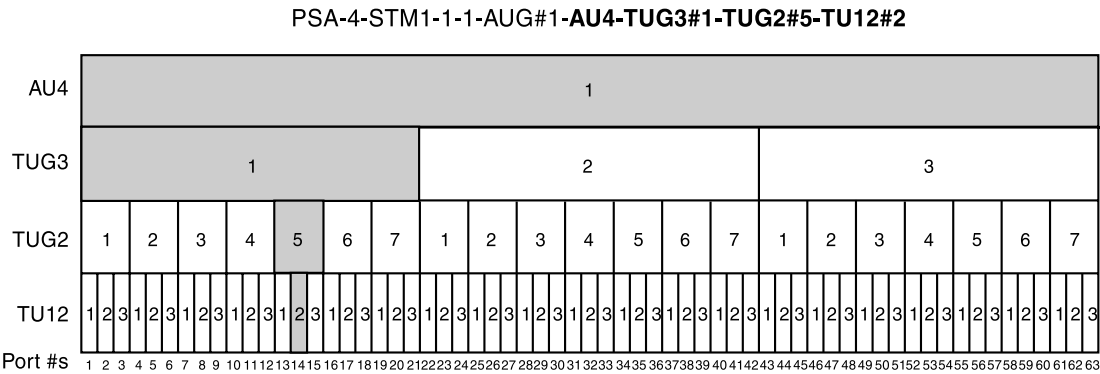
1. s = subrack number, u = unit number, p = port number
2. The square brackets indicate values that the system adds automatically. When you specify the value ALL for a field in the entity ID, the system automatically enters the value ALL for all subsequent fields in the entity ID.
3. These forms cannot be used when changing from AU4 clear channel (not TUG structured), because they do not specify how the other two TUG3s are to be multiplexed. For an STM-1 that is already TUG structured within the AU-4, any of the forms can be used, but only the form that specifies all TUG3s can be used when changing from AU-4 clear channel.

Illustration of signal layer addresses



**Graphical representation
of wideband signal**

The following illustration shows a graphical representation of a
wideband signal.



Wildcard addresses

About wildcards Rather than entering entity addresses individually, you can use a wildcard to specify a range of addresses. To use a wildcard, select the value ALL for any field in the entity address. The system automatically assigns all subsequent entity address fields the value ALL.

Examples The following are examples of entity addresses that use wildcards:

- MS-3-BSSU-ALL queries all the BSSUs on the MS-3 subrack.
- PSC-4-ALL-ALL-ALL queries all units, unit numbers, and ports on subrack PSC-4.
- ALL-ALL-ALL-ALL-ALL queries all units, unit numbers, and ports in all subracks in the system.



256 and 512 addressing

Differences between 256 and 512

On the user-interface windows, the port subracks on a 256 STM-1 equivalent system are numbered 4–11. The port subracks on a 512 STM-1 equivalent system are numbered 4–19.

Example

The following table describes the differences between the addressing on a 256 system and a 512 system.

System capacity	Address example
256	PSA-{4–11}-STM1-1
512	PSA-{4–19}-STM1-1

Related topic

For more information about 256 and 512 configurations, see “System capacity” (1-5).



MC entity addresses

Table of MC entity addresses

The following table shows the entity addresses for the Main Controller (MC) subrack.

Subrack type	Subrack number	Unit type	Unit number	Port number
MC	1, 2	MPU	1	N/A
		MSU	1	N/A
		LHU	1, 2	1–12
		ARU	1	N/A
		PSP	1	N/A



MS entity addresses

Table of MS entity addresses

The following table shows the entity addresses for the Matrix and Synchronisation (MS) subrack.

Subrack	Unit type	Unit number	Port number
MS-3	SRC	1, 2	N/A
	BSC	1, 2	N/A
	OLU	1–4	BSFI{1–5}
	BSSU	1–10	ECI{1–16}, BSFI{W, P}
	STU	1, 2	N/A



PSA entity addresses

Table of PSA entity addresses for the Physical ID

The following table shows the entity addresses for the Physical ID of a Port Subrack A (PSA).

Subrack type	Subrack number	Unit type	Unit number	Port number
PSA	4–11 or 4–19	SRC	1	N/A
		DTU	1, 2	N/A
		BSIU	1–10	ECI {1, 2}
		STM1	1–9, 11–19	1–4
			GRP1, GRP2	N/A
			MSP1, MSP3, MSP5, MSP7, MSP11, MSP13, MSP15, MSP17	1–4
		IU	1–8, 11–18	1–4

Table of PSA entity addresses for the Signal ID

The following table shows the entity addresses for the Signal ID of a Port Subrack A (PSA). In a PSA subrack, you can provision a Signal ID only for STM-1 ports.

AUG1	AU	TUG3	TUG2	TU12
AUG1#1	AU4	N/A	N/A	N/A
		TUG3#1, TUG3#2, TUG3#3	TUG2#1, TUG2#2, TUG2#3, TUG2#4, TUG2#5, TUG2#6, TUG2#7	TU12#1, TU12#2, TU12#3
			TU3	N/A
	AU3#1, AU3#2, AU3#3	N/A	N/A	N/A

PSC entity addresses

Table of PSC entity addresses for the Physical ID

The following table shows the entity addresses for the Physical ID of a Port Subrack C (PSC).

Subrack type	Subrack number	Unit type	Unit number	Port number
PSC	4–11 or 4–19	SRC	1	N/A
		DTU	1, 2	N/A
		BSIU	1–10	ECI {1, 2}
		STM16	1–8	1
			MSP1, MSP3, MSP5, MSP7	1
		STM4	1–8	1–4
			MSP1, MSP3, MSP5, MSP7	1–4

Table of STM-16 entity addresses for the Signal ID

The following table shows the STM-16 entity addresses for the Signal ID of a Port Subrack C (PSC).

AUG4	AUG1	AU	TUG3	TUG2	TU12
AUG4#1, AUG4#2, AUG4#3, AUG4#4	N/A	AU4_4c	N/A	N/A	N/A
	AUG1#1, AUG1#2, AUG1#3, AUG1#4	AU4	N/A	N/A	N/A
			TUG3#1, TUG3#2, TUG3#3	TUG2#1, TUG2#2, TUG2#3, TUG2#4, TUG2#5, TUG2#6, TUG2#7	TU12#1, TU12#2, TU12#3
				TU3	N/A
	N/A	AU3#1, AU3#2, AU3#3	N/A	N/A	N/A

Table of STM-4 entity addresses for the Signal ID

The following table shows the STM-4 entity addresses for the Signal ID of a Port Subrack C (PSC).

AUG4	AUG1	AU	TUG3	TUG2	TU12
AUG4#1	N/A	AU4_4c	N/A	N/A	N/A
	AUG1#1, AUG1#2, AUG1#3, AUG1#4	AU4	N/A	N/A	N/A
			TUG3#1, TUG3#2, TUG3#3	TUG2#1, TUG2#2, TUG2#3, TUG2#4, TUG2#5, TUG2#6, TUG2#7	TU12#1, TU12#2, TU12#3
				TU3	N/A
	N/A	AU3#1, AU3#2, AU3#3	N/A	N/A	N/A



Equipment protection group addresses

About equipment protection group addresses

The user interface uses GRP addresses to refer to entities that belong to equipment protection groups. The GRP address refers to *both* the working and protection units in an equipment protection group.

GRP address table

The following table lists GRP addresses.

Subrack and unit	Group
MS-3-SRC-{1, 2}	GRP
MS-3-BSSU-{1–10}	GRP
PSA-{4–11, 4–19}-DTU-{1, 2}	GRP
PSA-{4–11, 4–19}-STM1-{1–9}	GRP1
PSA-{4–11, 4–19}-STM1-{11–19}	GRP2
PSC-{4–11, 4–19}-DTU-(1, 2)	GRP

Example of a GRP address

The following is an example of a protection group:

- MS-3-SRC-1 = working unit
- MS-3-SRC-2 = protection unit
- MS-3-SRC-GRP = both the working and protection units



MSP addresses

About MSP addresses

A Multiplex Section Protection (MSP) group is a pair of STM-1, STM-4, or STM-16 ports that are provisioned for MSP. The user interface uses MSP addresses to refer to entities that belong to MSP protection groups. The MSP in the address refers to *both* the working and protection ports in an MSP protection group.

MSP address table

The following table lists MSP addresses.

Subrack and unit	Group	Port
PSA-{4-11, 4-19}-STM1	MSP{1, 3, 5, 7, 9, 11, 13, 15, 17}	1-4
PSC-{4-11, 4-19}-{STM16, STM4}	MSP{1, 3, 5, 7}	1

Example of an MSP address

The following is an example of an MSP protection group:

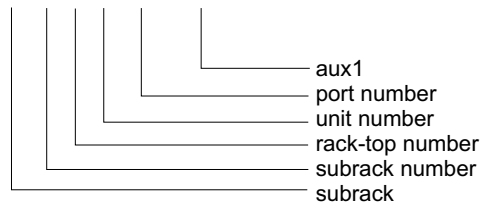
- PSA-1-STM1-1-1 = working port
- PSA-1-STM1-2-1 = protection port
- PSA-1-STM1-MSP1-1 = both the working and protection ports



RT addresses

About RT addresses Certain types of alarms display a rack-top (RT) entity address. The following illustration describes the rack-top address.

MC-1-RT-1-{1, 2}-{1, 2}



Port number and aux1 table The following table describes the port number and aux1 values.

Port number	Aux1
1 = rack-top battery input	1 = battery input A 2 = battery input B
2 = rack-top fuse array	1 = fuse 1 2 = fuse 2



Fibre addresses

About fibre addresses

Fibre addresses are displayed after a query from the View Current Alarms window, *Alarms > View Current Alarms*, for the following alarms:

- CABLEcEQ
- CABLEcTIM
- INTFcEQ

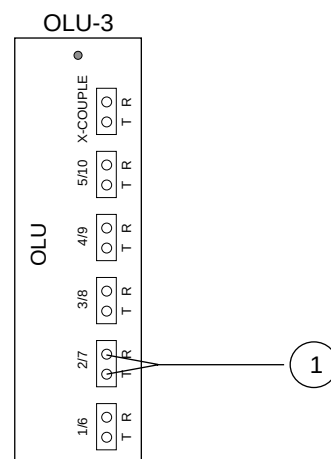
You can also enter fibre addresses from the Fibre Assignments window, *Utilities > Fibre Assignments*.

The following table displays all possible fibre addresses.

Subrack type	Subrack number	Unit type	Unit number	Port number
MS	3	OLU	1–4	BSFI{1–5}
		BSSU	1–10	BSFI{W, P}
PSA	4–11 or 4–19	BSIU	1–10	ECI{1, 2}
PSC	4–11 or 4–19	BSIU	1–10	ECI{1–4}

Example of a fibre address

The following illustration shows the physical port associated with the fibre address MS-3-OLU-3-BSFI2.



Legend:

1. Port 2 (BSFI2) on OLU-3





6 About alarms

Overview

Purpose “About alarms” contains general information about alarms.

Organisation “About alarms” is organised as follows:

- “Alarm terms” (6-2)
- “Defects and failures” (6-3)
- “Delay timers” (6-4)
- “Alarm Panel” (6-5)
- “User Panel” (6-6)
- “Conditions that affect service” (6-7)
- “Alarm indicator definition” (6-8)
- “Alarm indicator descriptions” (6-9)
- “MDIs and MDOs” (6-10)
- “About disconnecting and suppressing alarm indicators” (6-12)
- “About provisioning alarm indicators” (6-13)



Alarm terms

- List of terms**
- Deferred** Deferred indicates one, or both, of the following: a performance-degrading condition exists, but the condition does not affect service; a changeover to standby equipment has been used to restore service. Maintenance personnel must take immediate action, but they must resolve any prompt alarms first.
- Information** An alarm designated as information means that the alarm requires no immediate action. Maintenance personnel can perform the required actions on a scheduled basis or after an accumulation of maintenance events. Information alarms are indicated only on the User Panel.
- Prompt** A prompt alarm indicates that maintenance personnel must repair the defective equipment or take whatever corrective action is necessary to restore good service. Alarms for conditions that affect service are always classified as prompt.



Defects and failures

Differences between transmission and equipment defects or failures

The system collects information about transmission and equipment defects, failures, or degraded performance.

The difference between a transmission defect or failure, and an equipment defect or failure is as follows:

- A transmission defect or failure indicates a problem with the transmission signal received from outside your local equipment.
- An equipment defect or failure indicates a problem with the system equipment.

Alarm and defect reports

The system logs information about transmission and equipment defects and alarms. You can examine or print a report from a local or remote PC.

How the system correlates defects

The system correlates observed defects to determine the source of the trouble. If multiple parts of the system detect defects caused by one problem, the system uses defect correlation to try to find the real cause and to suppress side-effect causes. After the system correlates a defect, the system will time the defect to determine if the defect should be declared a failure.

Failures and consequent actions

If a defect persists long enough to be considered a failure, the system initiates the consequent actions defined for that failure. Consequent actions return the system to proper operation or prevent faults from propagating through the network.

Example of a consequent action

One example of a consequent action is the switching of service from the equipment that is currently providing service to standby or protection equipment.



Delay timers

Defect-to-alarm delay timers

The defect-to-alarm delay is the amount of time the system waits after a defect occurs before the system declares and reports a failure. If the defect goes away before the defect-to-alarm delay expires, no alarm is generated.

Alarm-clear delay timers

The alarm-clear delay is the number of seconds that the system waits after an equipment or transmission alarm has cleared before turning off the associated alarm indicators and generating an alarm-clear message.



Alarm Panel

Illustration The following illustration shows the Alarm Panel.



What is displayed on the Alarm Panel?

The Alarm Panel displays alarm tallies and information about autonomous events. You can gain access to the Alarm Panel from a local or remote PC.

What are alarm tallies?

Alarm tallies are the current numbers of prompt, deferred, and information alarms for the system.

What are autonomous events?

Autonomous events are actions that the system initiates automatically.

Examples of autonomous events

Alarms, protection-switching events, and system clock reference changes are examples of autonomous events.



User Panel

User Panel alarm indicators and controls

The User Panel is located on the front of the Main Controller rack, below the Main Controller subrack. The User Panel displays general system status and alarm information.

The Alarm Connector Panel (ACP) and the Fan Connector Panel (FCP) are located on the back of the User Panel. The ACP and the FCP have connectors for alarm-related cables.

Related topics

For more information, see one of the following topics:

- “User Panel” (1-20)
- “Alarm Connector Panel (ACP)” (1-22)
- “Fan Connector Panel (FCP)” (1-25)



Conditions that affect service

- What affects service?** Any of the following conditions will affect service:
- Protection is not available for the alarmed equipment or transmission entity.
 - The alarmed entity is still providing service and cannot be protected.
 - For control functions, any condition that can cause a cross-connect command to be denied.



Alarm indicator definition

What are alarm indicators?

Once a failure is declared, the system raises an alarm and turns on the appropriate alarm indicators. The alarm indicators provide a *trail of lights* that identifies the suite, rack, and unit on which the failure occurred. Alarm indicators are interfaced through solid-state relays located on the ARU in the Main Controller subrack. Alarm indicators are turned on or off by opening or closing relay contacts. When the condition that caused an alarm clears, the system clears the failure and automatically turns the alarm indicators off.



Alarm indicator descriptions

End-of-suite alarm indicators

Typically, Prompt and Deferred end-of-suite alarm indicators are located at the end of every suite (aisle), and are activated when the system detects a fault in that suite. You can disconnect or suppress end-of-suite alarm indicators from the User Panel or from a local or remote PC.

Rack-top alarm indicators

Prompt and Deferred rack-top alarm indicators are located at the top of each equipment rack and are activated when the system detects a fault in that rack. You can suppress rack-top alarm indicators from the User Panel or from a local or remote PC. You cannot disconnect rack-top alarm indicators.

Station alarm indicators

Station alarm indicators are alarm indicators that your company has designed to draw attention to an alarm condition. Station alarm indicators can be designed to either ring or light. These alarm indicators can be located in the equipment room or in other parts of the office. The system provides relays for the disconnectable and nondisconnectable station alarm indicators.

Disconnectable and nondisconnectable station alarm indicators

In a typical configuration, disconnectable station alarm indicators are connected to audible alarms, and nondisconnectable station alarm indicators are connected to visual alarms. If you disconnect a station alarm indicator, the audible alarms are silenced, but the visual alarms remain active until the failure has cleared.

You can disconnect or suppress disconnectable station alarm indicators on a system-wide basis. You cannot disconnect nondisconnectable station alarm indicators, but you can suppress nondisconnectable station alarm indicators on a system-wide basis.

You can disconnect or suppress station alarm indicators from the User Panel or from a local or remote PC.

Related topic

For information about Miscellaneous Discrete (MD) alarm indicators, see “MDIs and MDOs” (6-10).



MDIs and MDOs

- Description** Miscellaneous Discrete (MD) alarm indicators provide alarm indications for internal and external events; such as burglar alarms, smoke detectors, door contacts, and fan failures in port racks that are equipped with PSC subracks. MD alarm indicators are connected on the Fan Connector Panel (FCP), which is located on the back of the User Panel. The system provides Miscellaneous Discrete Inputs (MDIs) and Miscellaneous Discrete Outputs (MDOs).
- MDIs** MDIs provide inputs to the DACS system from fan trays in port racks that are equipped with PSC subracks, and from external equipment. You can use MDIs to collect status information from other transmission equipment or to monitor internal and external events. The DACS system allows up to eight inputs from fan trays in port racks that are equipped with PSC subracks, and up to four inputs from external equipment.
- MDOs** You can use MDOs to provide outputs from the DACS system to drive external equipment. The DACS system allows three MDOs.

Connecting MDIs to the FCP MDIs from external equipment are connected to the connector labeled MD IN on the FCP. Refer to “Fan Connector Panel (FCP)” (1-25) for a description and illustration of the FCP.

MDIs from fan trays in port racks that are equipped with PSC subracks are connected to the connectors labeled MDI 1 through MDI 4 on the FCP. Each of the four MDIs is a group of four connectors, for a total of 16 connectors. This configuration gives you flexibility in connecting the MDIs.

If you want to use MDIs to monitor fan failures and external equipment alarms and you have more than four MDIs, group the fan tray inputs, because fan failures are also indicated by lighting an LED on the connector panel of the failed port rack fan tray. If fan tray MD inputs are grouped and one of the fans in the group fails, you can identify which port rack fan tray has the failure by looking for a lighted FAIL LED on each fan tray connector panel.

MDI connection example If you have four port rack fan trays that you want to connect to MDIs, you can connect all four fan trays to one MDI, one fan tray to each of the four MDIs, or two fan trays to two of the four MDIs. If you have more than four port rack fan trays, more than one fan tray will have to be connected to at least one MDI.

- Provisioning MDs** You cannot enable or disable MDs from the user interface on the DACS system. MDs are always enabled.
- Testing MDOs** You can test the MDO alarm indicators from the *Maintenance > Alarm Indicator Tests* window. If the MDOs are not connected to any external equipment, you can run an Alarm Indicator test and check for continuity on a specific output with a Volt Ohm Meter (VOM).
- Testing MDIs** All MDIs were tested during installation. If you need to test the MDIs again, you can short the appropriate pins and check for an alarm indication. You can also run a diagnostic test on the MD input circuitry on the ARU using the MD Inputs diagnostic test.
- Related topic**
Use the *Maintenance > Execute Tests > Diagnostic Tests* window to run an MD Inputs diagnostic test.
- Alarms on MDs** MDcIP{1–4} alarms report monitored internal or external events to the local system. If an event occurs, the system will raise an alarm. You can change the severity of these alarms.
- Related topic**
To change the alarm severity, go to *Provision > Alarm Settings > Severity Levels* on the user interface.



About disconnecting and suppressing alarm indicators

General information about disconnecting and suppressing alarm notifications

When you disconnect or suppress alarm indicators, the system will turn off the corresponding visual or audible notifications of the alarm. However, you can still gain access to information about alarms through a local or remote PC with XC-CIT application software. A yellow LED next to the DISCONNECTED or SUPPRESSED button on the User Panel indicates that alarm indicators are disconnected or suppressed.

About disconnecting alarm indicators

When you disconnect alarm indicators, the disconnection becomes a system-wide and permanent condition. Alarms that occur after you disconnect alarm indicators will not be indicated until you remove the disconnection.

You can remove the disconnection in either of the following ways:

- Press the DISCONNECT button on the User Panel
- Go to *Alarms > Station Alarm Control*

About suppressing alarm indicators

When you suppress alarm indicators, the suppression becomes a system-wide and temporary condition. The system will turn off suppressible indicators for current alarms only. Any subsequent alarms will light the alarm indicators. Once you suppress the alarm indicators, the SUPPRESSED alarm indicator on the User Panel lights and remains lit until you clear the originally-suppressed alarms. You must clear the originally-suppressed alarms to remove the suppression of any alarm indicators.



About provisioning alarm indicators

Changing alarm indicators You can change station, rack-top, end-of-suite, and User Panel alarm indicators from suppressible to nonsuppressible or vice versa by using the Alarm Suppress Control window at *Provision > Alarm Settings > Alarm Suppress Control*.





7 Alarms

Overview

- Purpose** This chapter contains the following information:
- Descriptions of the windows that appear from the Alarms menu
 - Step-by-step procedures for the following:
 - Querying all currently-active or selected alarms
 - Querying the current state of station alarms
 - Disconnecting, connecting, or suppressing station alarms
 - Displaying the Alarm Panel

For general information about alarms, see Chapter 6, “About alarms”.

- Organisation** The organisation is as follows:
- “View Current Alarms window and procedures” (7-2)
 - “Station Alarm Control window and procedures” (7-8)
 - “Display Alarm Panel and procedure” (7-12)



View Current Alarms window and procedures

Overview

Purpose Use the View Current Alarms window to query and display information about currently-active alarms.

Window location *Alarms > View Current Alarms*

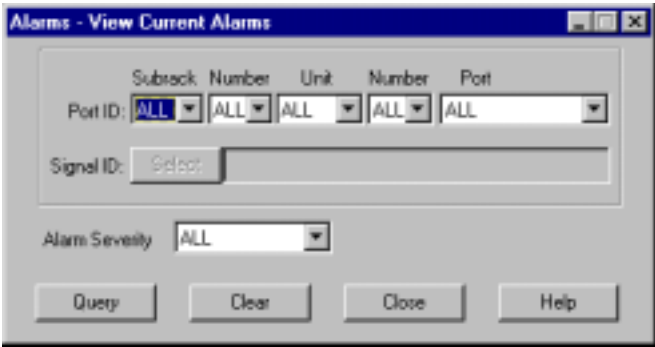
Organisation This section is organised as follows:

- [“View Current Alarms window description” \(7-3\)](#)
- [“Querying all currently active alarms” \(7-4\)](#)
- [“View Current Alarms query results” \(7-5\)](#)
- [“Querying selected alarms” \(7-7\)](#)



View Current Alarms window description

Illustration The following illustration shows the View Current Alarms window.



Field descriptions The View Current Alarms window has the following fields.

Field name	Description
Port ID	The Port ID fields specify the physical location of a port. The default value for the Port ID fields is ALL. For a description of the Port ID options, see “About physical layer addresses” (5-3).
Signal ID	The Signal ID field specifies the multiplexing structure for a signal. The default value for the Signal ID fields is ALL. For a description of the Signal ID options, see “About signal layer addresses” (5-4).
Alarm Severity	The Alarm Severity field specifies the severity of the alarms that you want to view. The valid values are the following: Prompt, Deferred, Info, ALL. The default value is ALL.

Related topic For general information about windows, see “About the main application window” (4-10).



Querying all currently active alarms

Procedure

- 1 Go to the View Current Alarms window at *Alarms > View Current Alarms*.
-

- 2 Click Query.

END OF STEPS



View Current Alarms query results

Illustration Use the following illustration only as an example of query results for the View Current Alarms window.

Query Completed 1999/03/01 12:10:25

	Date Set	Time Set	Equipment ID	Signal ID	Category	Failure Condition	Severity	Service Affecting
1	1999/03/01	12:10:25	P3A-5-3THL-4-1	A00#1-AU4-TU03#2-TU02#1-TU12#1	TRANSMISSION	MSCAIS	PROMPT	SA
2	1999/03/01	12:10:25	P3A-11-8THL-12-1	A00#1-AU4-TU03#1-TU02#1-TU12#2	EQUIPMENT	RSCLOF	DEFERRED	NSA
3	1999/03/01	12:10:25	P3A-7-3THL-6-2	A00#1-AU4-TU03#1-TU02#1-TU12#2	TRANSMISSION	A0CLOP	INFO	NSA

Buttons: Print, Close, Help

Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information is displayed for a View Current Alarms query.

Column	Description
Date Set	The Date Set column displays the date the system generated the alarm.
Time Set	The Time Set column displays the time the system generated the alarm.
Equipment ID	The Equipment ID column displays the physical location of the equipment you queried. For a description of the equipment addresses, see “About physical layer addresses” (5-3).
Signal ID	The Signal ID column displays the multiplexing structure of the alarmed transmission signal. For a description of the Signal ID options, see “About signal layer addresses” (5-4).
Category	The Category column displays the alarm category as Equipment or Transmission. For more information, see “Differences between transmission and equipment defects or failures” (6-3).

Column	Description
Failure Condition	The Failure Condition column displays the failure condition associated with the alarm. For more information about each of these failure conditions, see “Alarm list” (21-1).
Severity	The Severity column displays the alarm severity as Info, Deferred, or Prompt.
Service Affecting	The Service Affecting column displays the service-affecting status of the alarm as Service Affecting or Non-Service Affecting.

Related topic For general information about windows, see “About the main application window” (4-10).



Querying selected alarms

Procedure

- 1 Go to the View Current Alarms window at *Alarms > View Current Alarms*.
- 2 To query a specific port, select a value other than ALL for all Port ID fields. To query a specific signal ID at the selected port, specify a value for Signal ID.

Reference: For more information, see one of the following topics:

- “About physical layer addresses” (5-3)
- “About signal layer addresses” (5-4)

- 3 To query a specific severity level, select a value other than ALL for Alarm Severity.

- 4 Click Query.

END OF STEPS



Station Alarm Control window and procedures

Overview

- Purpose** Use the Station Alarm Control window to do the following:
- Query the current state (Connected or Disconnected) of the station alarm indicators
 - Connect or disconnect station alarm indicators
 - Suppress alarm indicators for currently-active alarms.

Window location *Alarms > Station Alarm Control*

- Organisation** This section is organised as follows:
- “Station Alarm Control window description” (7-9)
 - “Querying the current state of the station alarms” (7-10)
 - “Disconnecting, connecting, or suppressing station alarms” (7-11)



Station Alarm Control window description

Illustration The following illustration shows the Station Alarm Control window.



Button descriptions The Station Alarm Control window has the following buttons.

Button name	Description
Disconnect Station Alarms	Clicking the Disconnect Station Alarms button disconnects the station alarm indicators. Station alarm indicators will <i>not</i> light or sound until they are once again connected by using the Connect Station Alarms button.
Connect Station Alarms	Clicking the Connect Station Alarms button connects the station alarm indicators so that they will light or sound when a station alarm is active.
Suppress Station Alarms	The Suppress Station Alarms button causes a system-wide temporary suppression of current station alarm indicators. Clicking the Suppress Station Alarms button will <i>not</i> affect LED indicators on units and station alarm indicators that cannot be suppressed, nor will it affect indicators for future alarms.

Related topic For general information about windows, see “About the main application window” (4-10).



Querying the current state of the station alarms

Procedure

- 1 Go to the Station Alarm Control window at *Alarms > Station Alarm Control*.
-

- 2 Click Query.

Result:

The current state (Connected or Disconnected) of the station alarm indicators is displayed in a query results window.

END OF STEPS



Disconnecting, connecting, or suppressing station alarms

Procedure

- 1 Go to the Station Alarm Control window at *Alarms > Station Alarm Control*.
 - 2 Click Disconnect Station Alarms, Connect Station Alarms, or Suppress Station Alarms.
-

END OF STEPS



Display Alarm Panel and procedure

Overview

Purpose Use the Display Alarm Panel command to display the Alarm Panel. If the Alarm Panel is already displayed, this command restores the Alarm Panel to its default position. The default position for the Alarm Panel is the left side of the screen.

Window location *Alarms > Display Alarm Panel*



Displaying the Alarm Panel

Procedure

- 1 Go to the Alarms menu.
-

- 2 Select Display Alarm Panel.

END OF STEPS





8 Reports

Overview

- Purpose** “Reports” contains the following information:
- General information about reports
 - Descriptions of the windows that are used to request information for and to print reports
 - Step-by-step procedures for requesting information for reports

- Organisation** “Reports” is organised as follows:
- “Background information” (8-2)
 - “Autonomous Messages window and procedures” (8-8)
 - “Performance Monitoring window and procedures” (8-25)
 - “User Transactions window and procedures” (8-34)
 - “Defects window and procedures” (8-39)



Background information

Overview

Purpose This section contains background information about reports.

Organisation This section is organised as follows:

- “About reports” (8-3)
- “Saving a report” (8-5)
- “Printing a report” (8-6)
- “Finding specific information in a report” (8-7)



About reports

What are reports? Use the report windows to query the system about user-initiated and system-initiated events that have occurred on the system over a period of time.

Which report window should I use? The following table shows which report window to use for each report type.

Report Type	Report Window
Alarms	Autonomous Messages
Protection switches	Autonomous Messages
System clock reference switches	Autonomous Messages
Threshold crossing alerts	Autonomous Messages
Unit state changes	Autonomous Messages
Port state changes	Autonomous Messages
Background diagnostic test completion messages	Autonomous Messages
User interface commands executed by a user	User Transactions
Performance monitoring data	Performance Monitoring
Equipment and transmission defects	Defects

How many records can the report log hold? The system collects information for the Autonomous Messages, User Transactions, and Defects reports, and stores the information in report logs. The Autonomous Messages and User Transactions report logs can each hold up to 5,000 records. The Defects report log can hold up to 1,000 records.

The report logs are circular, meaning that the system will delete the first (oldest) record in the log to make room for the 5,001st (1,001st for the Defects report log) record. The system deletes records only when the number of records exceeds the 5,000-record (1,000 for the Defects report log) limit.

How can you retrieve records after the system date and time have been changed?

When the system collects information for a report, it stamps each record with the system date and time before storing the record in the database. If the system date and time has been changed to a date and time that is in the distant future or past, and information is collected and stamped with that date and time, you may not be able to retrieve that information using a typical database query. To retrieve database records that have been stamped with a date and time that is in the distant future or past, specify the largest possible interval for your query.



Saving a report

Procedure After performing a query from any of the Reports windows, do the following on the Query Results window to save the query results to a file.

1 Click File.

2 Select Save As.

3 Specify a file name, and select one of the following file types:

- Worksheet file (*.xls)
- Tabbed text (*.txt)
- HTML file (*.html)
- All files (*.*)

If you save the information in the Query Results window as a Worksheet file (*.xls), you can modify this information using *Microsoft*[™] Excel.

END OF STEPS



Printing a report

Procedure After performing a query from any of the Reports windows, do the following to print the query results.

- 1** Click Print.

- 2** Select the appropriate printer options.

- 3** Click OK.

END OF STEPS



Finding specific information in a report

Procedure After performing a query from any of the Reports windows, do the following to find specific information in the query results.

1 Click Edit.

2 Click Find.

3 Specify what to find.

4 Click Find.

5 Perform another search or click Close to close the Find window.

END OF STEPS



Autonomous Messages window and procedures

Overview

Purpose Use the Autonomous Messages window to query or print information about autonomous messages or events. Autonomous events are actions that the system initiates automatically. The system generates an autonomous message for every autonomous event. Alarms, protection-switching events, and system clock reference changes are examples of autonomous events.

Window location *Reports > Autonomous Messages*

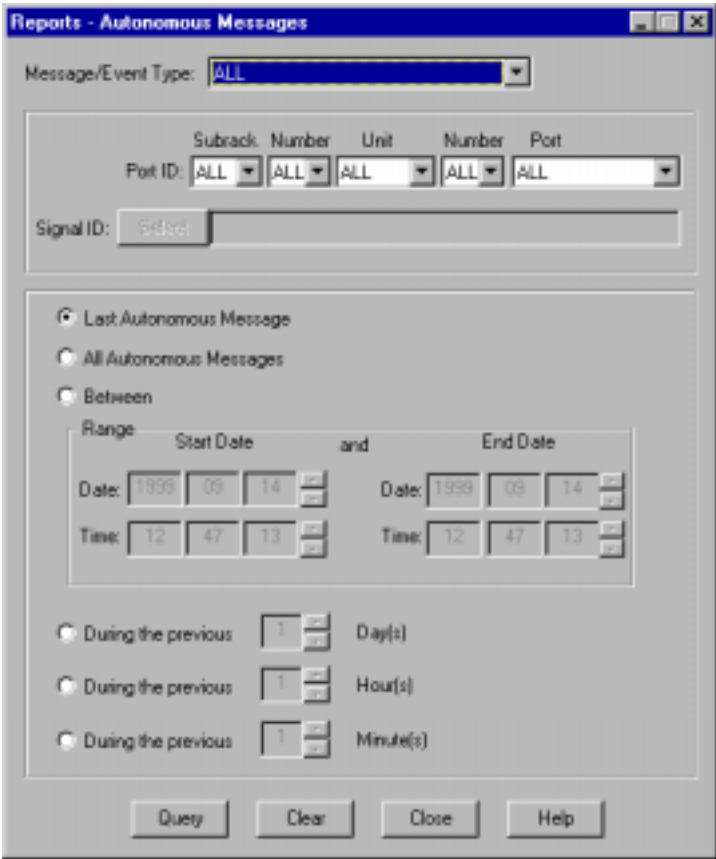
Organisation This section is organised as follows:

- [“Autonomous Messages window description” \(8-9\)](#)
- [“Querying the last autonomous message” \(8-12\)](#)
- [“Querying all autonomous messages” \(8-13\)](#)
- [“Querying autonomous messages by specifying a time” \(8-14\)](#)
- [“Querying autonomous messages by specifying a message type or entity” \(8-15\)](#)
- [“Autonomous Messages query results” \(8-16\)](#)
- [“ALL query results” \(8-17\)](#)
- [“Alarms query results” \(8-18\)](#)
- [“Diagnostic Tests Completion Messages query results” \(8-19\)](#)
- [“Protection Switch Events query results” \(8-20\)](#)
- [“System Clock Reference Changes query results” \(8-21\)](#)
- [“Threshold Crossing Alerts query results” \(8-22\)](#)
- [“Unit State Changes query results” \(8-23\)](#)
- [“Port State Changes query results” \(8-24\)](#)



Autonomous Messages window description

Illustration The following illustration shows the Autonomous Messages window.



Field descriptions The Autonomous Messages window has the following fields.

Field name	Description
Message/Event Type	The Message/Event Type field specifies the type of autonomous message or event. The values are as follows: • ALL — Summary information about all autonomous messages or events • Alarms • Diagnostic Test Completion Messages — Information about diagnostic tests that were run in the background. • Protection Switch Events • System Clock Reference Changes • Threshold Crossing Alerts • Unit State Changes • Port State Changes
Port ID	The Port ID fields specify the physical location of a port. For a description of the Port ID options, see “About physical layer addresses” (5-3).
Signal ID	The Signal ID field specifies the multiplexing structure of a transmission signal. For a description of the Signal ID options, see “About signal layer addresses” (5-4).
Last Autonomous Message	Selecting the Last Autonomous Message field requests information about the most recent autonomous message or event. This field is selected by default when you open the Autonomous Messages window.
All Autonomous Messages	Selecting the All Autonomous Messages field requests information about all autonomous messages or events.
Between	Selecting the Between field requests information about the autonomous messages or events that occurred between the start and end dates and times that you specify. The date and time associated with an autonomous message or event is the system date and time, not the PC date and time.

Field name	Description
During the previous Day(s)	Selecting the During the previous Day(s) field requests information about the autonomous messages or events that occurred during the previous number of days that you specify. The values are 1–999.
During the previous Hour(s)	Selecting the During the previous Hour(s) field requests information about the autonomous messages or events that occurred during the previous number of hours that you specify. The values are 1–48.
During the previous Minute(s)	Selecting the During the previous Minute(s) field requests information about the autonomous messages or events that occurred during the previous number of minutes that you specify. The values are 1–120.

Related topic For general information about windows, see “About the main application window” (4-10).



Querying the last autonomous message

Procedure

- 1 Go to the Autonomous Messages window at *Reports > Autonomous Messages*.
-

- 2 Click Query.

Last Autonomous Message is the default.

END OF STEPS



Querying all autonomous messages

Procedure

- 1** Go to the Autonomous Messages window at *Reports > Autonomous Messages*.
- 2** Select All Autonomous Messages.
- 3** Click Query.

END OF STEPS



Querying autonomous messages by specifying a time

Procedure Use the following procedure to query autonomous messages by specifying a range of dates or the number of days, hours, or minutes.

- 1** Go to the Autonomous Messages window at *Reports > Autonomous Messages*.
-

2

If	Then
You want to specify a range of dates	1. Click Between. 2. Select a Start Date and an End Date.
You want to specify the number of days, hours, or minutes	Select one of the following: • During the previous Day(s) • During the previous Hour(s) • During the previous Minute(s)

- 3** Click Query.

END OF STEPS



Querying autonomous messages by specifying a message type or entity

Procedure

- 1 Go to the Autonomous Messages window at *Reports > Autonomous Messages*.
-

2	<table><tr><th>If</th><th>Then</th></tr><tr><td>You want to query a specific message or event type</td><td>Select a Message/Event Type.</td></tr><tr><td>You want to query a specific entity</td><td>Select the Port ID and if applicable, the Signal ID. Use ALL to query more than one signal level or piece of equipment. For more information, see “Wildcard addresses” (5-9).</td></tr></table>	If	Then	You want to query a specific message or event type	Select a Message/Event Type.	You want to query a specific entity	Select the Port ID and if applicable, the Signal ID. Use ALL to query more than one signal level or piece of equipment. For more information, see “Wildcard addresses” (5-9).
If	Then						
You want to query a specific message or event type	Select a Message/Event Type.						
You want to query a specific entity	Select the Port ID and if applicable, the Signal ID. Use ALL to query more than one signal level or piece of equipment. For more information, see “Wildcard addresses” (5-9).						

- 3 Click Query.

END OF STEPS



Autonomous Messages query results

Illustration Use the following illustration only as an example of query results for the Autonomous Messages window.

	Date of Event	Time of Event	Event Type	Entity ID	Parameters
1	1999/03/01	12:32:32	DIAG_TEST	PSA-5-STMI-4-1	INTERNAL Unit 5
2	1999/03/01	12:32:32	SWITCH_EQP	PSA-5-STMI-4-1	Force Switch to Protection

Important! The data displayed on this screen may *not* be typical.

Message/Event Type query results

The Autonomous Message Query Results window displays the following Event Types:

- “ALL query results” (8-17)
- “Alarms query results” (8-18)
- “Diagnostic Tests Completion Messages query results” (8-19)
- “Protection Switch Events query results” (8-20)
- “System Clock Reference Changes query results” (8-21)
- “Threshold Crossing Alerts query results” (8-22)
- “Unit State Changes query results” (8-23)
- “Port State Changes query results” (8-24)

Related topic

For general information about windows, see “About the main application window” (4-10).



ALL query results

Results field descriptions for an All query

The following information is displayed for an autonomous message or event type all query.

Column	Description
Date of Event	The Date of Event column displays the date of the autonomous event.
Time of Event	The Time of Event column displays the time of the autonomous event.
Event Type	The Event Type column displays these messages when the following system-initiated events occur: • SYS_CLK_REF_SWITCH — the system clock reference has changed • SWITCH_EQP — an equipment protection switching event has occurred • SWITCH_MSP — a Multiplex Section Protection (MSP) switching event has occurred • SWITCH_SNCP — a Sub-Network Connection Protection (SNCP) switching event has occurred. • TCA — a threshold crossing alert has occurred • ALM_BNDL — alarms were raised or were cleared • DIAG_TEST — a diagnostic test was run in the background • MODE_CHG — the monitoring state of a port has changed • STATE_CHG — the state of a controller or a unit has changed or the controller/unit was initialised
Entity ID	The Entity ID column displays the physical location of the signal or equipment associated with your query. For a description of the entity IDs, see “About physical layer addresses” (5-3).
Parameters	The Parameters column displays a summary of the events for the specified Event Type. If you need more information, query the specific event type. For example: from the Autonomous Messages window, select Protection Switch Events in the Message/Event Type column for detailed information about protection switching events.



Alarms query results

Results field descriptions for an Alarms query

The following information is displayed for an Alarms message or event type query.

Column	Description
Date Set	The Date Set column displays the date the system generated the alarm.
Time Set	The Time Set column displays the time the system generated the alarm.
Date Clear	The Date Clear column displays the date the alarm cleared.
Time Clear	The Time Clear column displays the time the alarm cleared.
Equipment ID	The Equipment ID column displays the physical location of the alarmed equipment. For a description of the equipment addresses, see “About physical layer addresses” (5-3).
Signal ID	The Signal ID column displays the multiplexing structure of the alarmed transmission signal. For a description of the Signal ID options, see “About signal layer addresses” (5-4).
Category	The Category column displays the alarm category as Equipment or Transmission. For more information, see “Differences between transmission and equipment defects or failures” (6-3).
Condition	The Condition column displays the failure condition associated with the alarm. For more information about each of these failure conditions, see “Alarm list” (21-1).
Status	The Status column displays the alarm status as Set or Clear. Set means that the alarm is active and it has not yet been cleared. Clear means that the alarm has been cleared.
Severity	The Severity column displays the alarm severity as Info, Deferred, or Prompt.
SA Status	The SA Status column displays the service-affecting status of the alarm as Service Affecting or Non-Service Affecting.



Diagnostic Tests Completion Messages query results

Results field descriptions for a Diagnostic Tests Completion Messages query

The following information is displayed for a Diagnostic Tests Completion Messages query. This screen will display the diagnostic tests that were run in the background.

Column	Description
Command	The Command column displays the command name as Execute Diagnostics.
Device EID	The Device EID column displays the physical location of the tested equipment. For a description of the equipment addresses, see “About physical layer addresses” (5-3).
Test Type	The Test Type column displays the type of diagnostic test as Internal, External, or All.
Test	The Test column displays the name of the diagnostic test that was executed. This column displays the name of a specific diagnostic test or All.
Loop Count	The Loop Count column displays the number of times (1–25) the diagnostic test was executed.
Result	The Result column displays the result of the test as one of the following: • TEST_PASSED • PARTIAL_PASSED • TEST_FAILED • TEST_ERRORED
Date	The Date column displays the date the diagnostic test was executed.
Time	The Time column displays the time the diagnostic test was executed.



Protection Switch Events query results

Results field descriptions for a Protection Switch Events query

The following information is displayed for an autonomous message or event type Protection Switch Events query.

Column	Description
Date of Event	The Date of Event column displays the date the protection switch occurred.
Time of Event	The Time of Event column displays the time the protection switch occurred.
Protection Group ID	The Protection Group ID column displays the physical location of the protection group. For a description of the protection group addresses, see “About physical layer addresses” (5-3).
Current Request	The Current Request column displays the current protection state.



System Clock Reference Changes query results

Results field descriptions for a System Clock Reference Changes query

The following information is displayed for an autonomous message or event type System Clock Reference Changes query.

Column	Description
Date of Event	The Date of Event column displays the date the reference change occurred.
Time of Event	The Time of Event column displays the time the reference change occurred.
New Reference ID	The New Reference ID column displays the physical location of the new system clock input reference.
New Reference Number	The New Reference Number column displays the new system clock input reference number.
Old Reference ID	The Old Reference ID column displays the physical location of the old (previously active) system clock input reference.
Old Reference Number	The Old Reference Number column displays the old (previously active) system clock input reference number.
STU Unit	The STU Unit column displays the physical location of the STU Unit.



Threshold Crossing Alerts query results

Results field descriptions for a Threshold Crossing Alerts query

The following information is displayed for an autonomous message or event type Threshold Crossing Alerts query.

Column	Description
Date of TCA	The Date of TCA column displays the date the threshold-crossing alert occurred.
Time of TCA	The Time of TCA column displays the time the threshold-crossing alert occurred.
Entity ID	The Entity ID column displays the physical location of the monitored entity. For a description of the entity IDs, see “About physical layer addresses” (5-3).
Trail Type	The Trail Type column displays the signal level of the trail as RS, MS, VC4_4c, VC4, VC3 (HP), VC3 (LP), or VC12.
PM Parameter	The PM Parameter column displays the performance-monitoring parameter for which the Threshold Crossing Alert (TCA) occurred. Near-End (NE) parameters are calculated by the local network element; Far-End (FE) parameters are calculated by the network element at the other end of the transmission facility. This column displays one of the following values: • NE-BBE — Near-End Background Block Error • NE-ES — Near-End Errored Second • NE-SES — Near-End Severely-Errored Second • NE-UAS — Near-End Unavailable Second • FE-BBE — Far-End Background-Block Error • FE-ES — Far-End Errored Second • FE-SES — Far-End Severely-Errored Second • FE-UAS — Far-End Unavailable Second
Threshold	The Threshold column displays the current TCA threshold.
Interval	The Interval column displays the collection interval for the performance-monitoring counts as 15-minute or 24-hour.



Unit State Changes query results

Results field descriptions for a Unit State Changes query

The following information is displayed for an autonomous message or event type Unit State Changes query.

Column	Description
Date of Change	The Date of Change column displays the date the unit state change occurred.
Time of Change	The Time of Change column displays the time the unit state change occurred.
Unit ID	The Unit ID column displays the physical location of the unit. For a description of the Unit IDs, see “About physical layer addresses” (5-3).
New State	The New State column displays the new unit state. For more information, see “Unit states” (11-11).
Old State	The Old State column displays the old (previous) unit state. For more information, see “Unit states” (11-11).



Port State Changes query results

Results field descriptions for a Port State Changes query

The following information is displayed for an autonomous message or event type Port State Changes query.

Column	Description
Date of Change	The Date of Change column displays the date the port state change occurred.
Time of Change	The Time of Change column displays the time the port state change occurred.
Port ID	The Port ID column displays the physical location of the port. For a description of the Port ID options, see “About physical layer addresses” (5-3).
New Monitoring State	The New Monitoring State column displays the new monitoring state of the port.



Performance Monitoring window and procedures

Overview

Purpose Use the Performance Monitoring window to query or print performance-monitoring data.

The system uses Greenwich Mean Time (GMT) to collect and store performance-monitoring data, and uses local time to display the data.

Window location *Reports > Performance Monitoring*

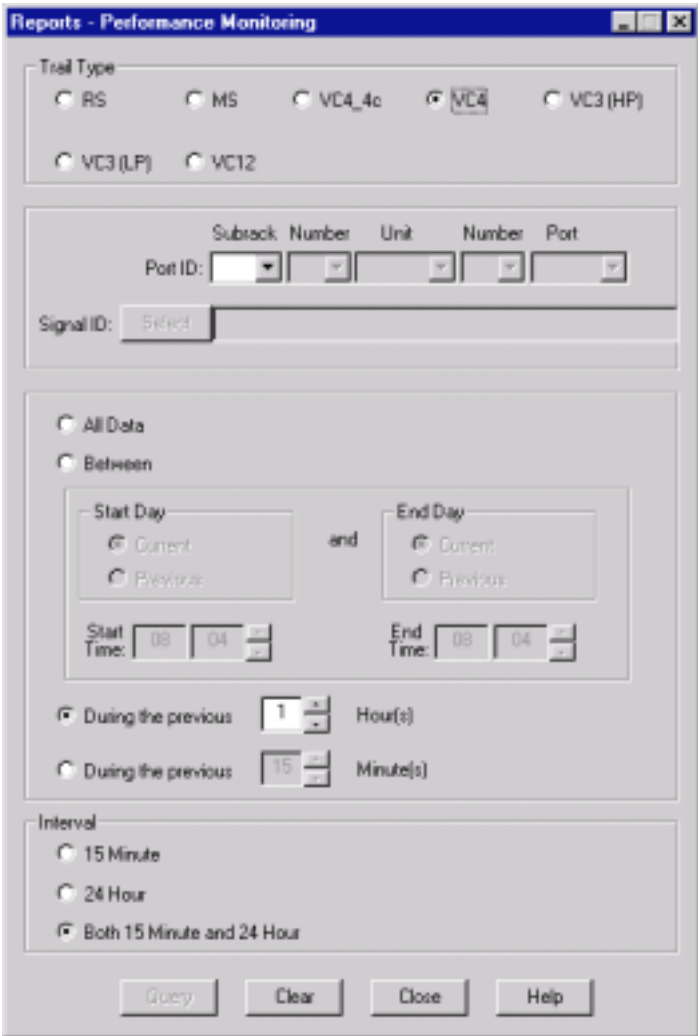
Organisation This section is organised as follows:

- “Performance Monitoring window description” (8-26)
- “Querying PM data” (8-29)
- “Performance Monitoring query results” (8-30)



Performance Monitoring window description

Illustration The following illustration shows the Performance Monitoring window.



Field descriptions The Performance Monitoring window has the following fields.

Field name	Description
Trail Type	Selecting a Trail Type field requests performance-monitoring data for that type of trail. The values are as follows: • RS • MS • VC4_4c • VC4 • VC3 (HP) — VC-3 as AU-3 • VC3 (LP) — VC-3 as TU-3 • VC12
Port ID	The Port ID fields specify the physical location of a port. For a description of the Port ID options, see “About physical layer addresses” (5-3).
Signal ID	The Signal ID field specifies the multiplexing structure of a transmission signal. For a description of the Signal ID options, see “About signal layer addresses” (5-4).
All Data	Selecting the All Data field requests all performance-monitoring data for the trail type and Signal ID that you specify. The system will report all 15-minute data that is in the database. The user interface will not allow you to specify an interval.
Between	Selecting the Between field requests performance-monitoring data collected between the dates and times that you specify.
Start Day	You can query the performance-monitoring data for a specific range of days starting with today or a previous day.
End Day	You can query the performance-monitoring data for a specific range of days ending with today or a previous day.
Start Time	You can query what performance-monitoring data the system collected starting at a specific time.
End Time	You can query what performance-monitoring data the system collected ending at a specific time.

Field name	Description
During the previous Hour(s)	Selecting the During the previous Hour(s) field requests performance-monitoring data collected during the previous number of hours that you specify. The values are 1–24.
During the previous Minute(s)	Selecting the During the previous Minute(s) field requests performance-monitoring data collected during the previous number of minutes that you specify. The values are 15–120, in 15-minute increments.
15 Minute	Selecting the 15 Minute field requests performance-monitoring data that was collected for a 15-minute interval.
24 Hour	Selecting the 24 Hour field requests performance-monitoring data that was collected for a 24-hour interval.
Both 15 Minute and 24 Hour	Selecting the Both 15 Minute and 24 Hour field requests performance-monitoring data that was collected for both 15-minute and 24-hour intervals.

Related topic For general information about windows, see “About the main application window” (4-10).



Querying PM data

Procedure

- 1 Go to the Performance Monitoring window at *Reports > Performance Monitoring*.
- 2 Select the Trail Type.
- 3 Select the Port ID.
- 4 Select the Signal ID if applicable.
- 5 Select one of the following fields:
 - All Data
 - Between, Start Day, End Day, Start Time, and End Time
 - During the previous Hour(s)
 - During the previous Minute(s)
- 6 Select one of the following fields:
 - 15 Minute
 - 24 Hour
 - Both 15 Minute and 24 Hour
- 7 Click Query.

END OF STEPS



Performance Monitoring query results

Illustration Use the following illustration only as an example of query results for the Performance Monitoring window.

	Date	Start Time	End Time	Entity ID	Trail Type	Parameter	Count	Interval	Status
1	1999/03/01	11:35:57	12:35:57	PSA-7-STEL-11-1-AUG#1-AU4	VC4	NE-E5	100	15-minute	Allow-Normal-Normal
2	1999/03/01	11:35:57	12:35:57	PSA-7-STEL-11-1-AUG#1-AU4	VC4	NE-SES	200	15-minute	Allow-Normal-Normal
3	1999/03/01	11:35:57	12:35:57	PSA-7-STEL-11-1-AUG#1-AU4	VC4	NE-UAS	300	15-minute	Allow-Normal-Normal
4	1999/03/01	11:35:57	12:35:57	PSA-7-STEL-11-1-AUG#1-AU4	VC4	NE-DSE	400	15-minute	Allow-Normal-Normal
5	1999/03/01	11:35:57	12:35:57	PSA-7-STEL-11-1-AUG#1-AU4	VC4	FE-E5	500	15-minute	Allow-Normal-Normal
6	1999/03/01	11:35:57	12:35:57	PSA-7-STEL-11-1-AUG#1-AU4	VC4	FE-SES	600	15-minute	Allow-Normal-Normal
7	1999/03/01	11:35:57	12:35:57	PSA-7-STEL-11-1-AUG#1-AU4	VC4	FE-UAS	700	15-minute	Allow-Normal-Normal
8	1999/03/01	11:35:57	12:35:57	PSA-7-STEL-11-1-AUG#1-AU4	VC4	FE-DSE	800	15-minute	Allow-Normal-Normal

Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the Performance Monitoring Query Results window.

Column	Description
Date	The Date column displays the date the performance-monitoring data was collected.
Start Time	The Start Time column displays the time the system started collecting performance-monitoring data.
End Time	The End Time column displays the time the system stopped collecting performance-monitoring data.
Entity ID	The Entity ID column displays the physical address of the monitored entity.
Trail Type	The Trail Type column displays the signal level of the trail as RS, MS, VC4_4c, VC4, VC3 (HP), VC3 (LP), or VC12.

Column	Description
Parameter	The Parameter column displays the performance-monitoring parameter for which the count was collected. Near-End (NE) parameters are calculated by the local network element; Far-End (FE) parameters are calculated by the network element at the other end of the transmission facility. This column displays one of the following values: • NE-BBE — Near-End Background-Block Error • NE-ES — Near-End Errored Second • NE-SES — Near-End Severely-Errored Second • NE-UAS — Near-End Unavailable Second • FE-BBE — Far-End Background-Block Error • FE-ES — Far-End Errored Second • FE-SES — Far-End Severely-Errored Second • FE-UAS — Far-End Unavailable Second
Count	The Count column displays the count for the corresponding performance-monitoring parameter.
Interval	The Interval column displays the collection interval for the performance-monitoring counts as 15-minute or 24-hour.
Status	The Status column has three parts: Count Control Status- Time Change Indication- Completeness. An example of the status of performance-monitoring data is Allow-Normal-Normal.
Status — Count Control Status	Part 1 of the Status column is the Count Control Status, and the values are as follows: • Allow — Performance-monitoring data collection has been enabled for the trail. • Inhibit — Performance-monitoring data collection has <i>not</i> been enabled for the trail.

Column	Description
Status — Time Change Indication	Part 2 of the Status column is the Time Change Indication, and the values are as follows: • Normal — The system time was not changed during the interval. Performance-monitoring data collection is complete for the entire interval, or complete up to the current time for the current interval. • Shortened — The time interval for which the counts were collected was shorter than the normal interval. This can happen if the system time was changed during the interval, or if the system makes an autonomous time adjustment. • Lengthened — The time interval for which the counts were collected was longer than the normal interval. This can happen if the system time was changed during the interval, or if the system makes an autonomous time adjustment.
Status — Completeness	Part 3 of the Status column is Completeness, and the values are as follows: • Normal — Performance-monitoring counts were collected for the entire interval. • Partial — Performance-monitoring counts were collected for only part of the specified interval. This can happen if a user allows or inhibits the counts during the interval, or if one or more of the conditions necessary for performance-monitoring counting changed during the interval. A protection switch on a transmission port is one example of a change that effects performance-monitoring counting. • Adjusted — Performance-monitoring counts were set to zero during the interval. This can happen if the counts were reset by a Clear Counters command or by a protection switch on a transmission port.

Related topic For general information about windows, see “About the main application window” (4-10).

**Time zones and 24-hour
intervals**

The system uses Greenwich Mean Time (GMT) to collect and store performance-monitoring data, and converts it to local time to display the data. This conversion is transparent to you when you request 15-minute intervals. However, when you request 24-hour intervals, this conversion may cause the system to display a greater date range, with a different start and end time than what you requested, depending on the times you specified.



User Transactions window and procedures

Overview

Purpose Use the User Transactions window to query or print information about user transactions. A user transaction is a user-initiated command, for example, disconnecting a cross connection. The system stores only information about user transactions that completed successfully.

Window location *Reports > User Transactions*

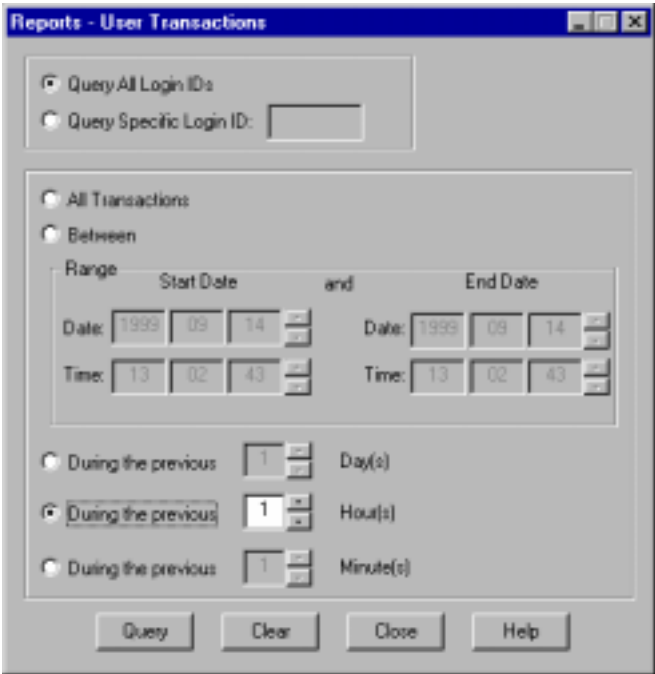
Organisation This section is organised as follows:

- [“User Transactions window description” \(8-35\)](#)
- [“Querying user transactions” \(8-37\)](#)
- [“User Transactions query results” \(8-38\)](#)



User Transactions window description

Illustration The following illustration shows the User Transactions window.



Field descriptions The User Transactions window has the following fields.

Field name	Description
Query All Login IDs	Selecting the Query All Login IDs field requests user transaction data for all login IDs.
Query Specific Login ID	Selecting the Query Specific Login ID field requests user transaction data for the specified login ID.
All Transactions	Selecting the All Transactions field requests information about all user transactions.
Between	Selecting the Between field requests information about user transactions that occurred between the dates and times that you specify.
During the previous Day(s)	Selecting the During the previous Day(s) field requests information about user transactions that occurred during the previous number of days that you specify. The values are 1–999.

Field name	Description
During the previous Hour(s)	Selecting the During the previous Hour(s) field requests information about user transactions that occurred during the previous number of hours that you specify. The values are 1–48.
During the previous Minute(s)	Selecting the During the previous Minute(s) field requests information about user transactions that occurred during the previous number of minutes that you specify. The values are 1–120.

Related topic For general information about windows, see “About the main application window” (4-10).



Querying user transactions

Procedure

- 1** Go to the User Transactions window at *Reports > User Transactions*.
-

- 2** Select one of the following fields:

- Query All Login IDs
 - Query Specific Login ID
-

- 3** Select one of the following fields:

- All Transactions
 - Between
 - During the previous Day(s)
 - During the previous Hour(s)
 - During the previous Minute(s)
-

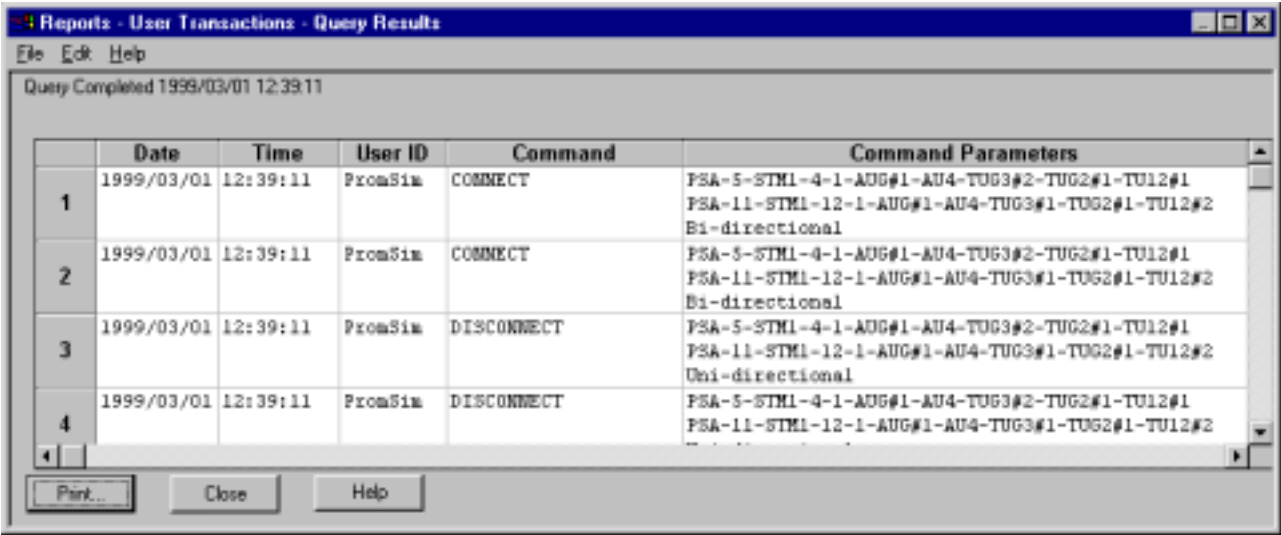
- 4** Click Query.

END OF STEPS



User Transactions query results

Illustration Use the following illustration only as an example of query results for the User Transactions window.



Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the User Transactions Query Results window.

Column	Description
Date	The Date column displays the date of the user transaction.
Time	The Time column displays the time of the user transaction.
User ID	The User ID column displays the User ID associated with the user transaction.
Command	The Command column displays the command that was executed by the user.
Command Parameters	The Command Parameters column displays parameters associated with the command that was executed by the user.

Related topic For general information about windows, see “About the main application window” (4-10).



Defects window and procedures

Overview

Purpose Use the Defects window to query or print information about equipment or transmission defects. The system stores only information about defects that do not become alarms.

Window location *Reports > Defects*

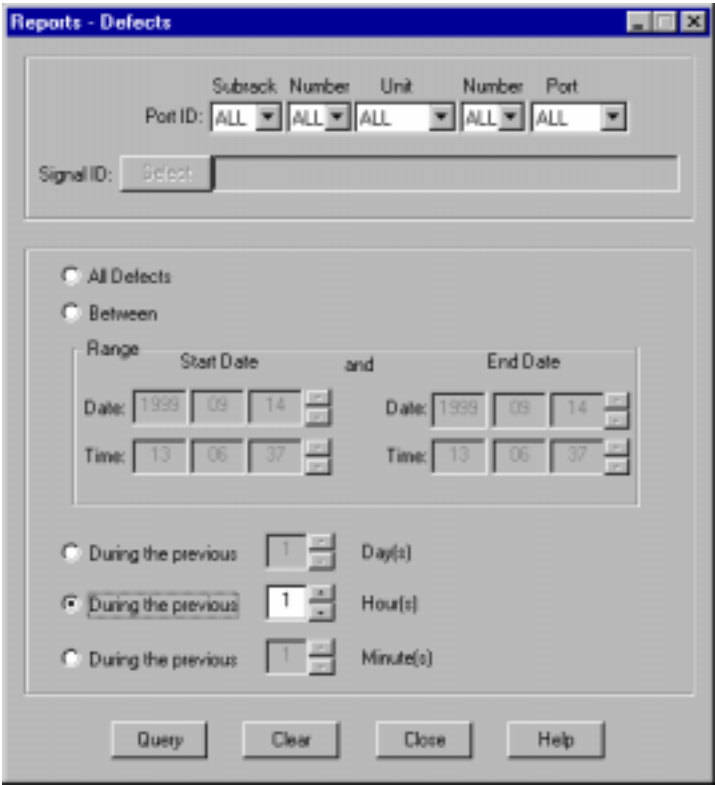
Organisation This section is organised as follows:

- “Defects window description” (8-40)
- “Querying defects” (8-42)
- “Defects query results” (8-43)



Defects window description

Illustration The following illustration shows the Defects window.



Field descriptions The Defects window has the following fields.

Field name	Description
Port ID	The Port ID fields specify the physical location of a port. For a description of the Port ID options, see “About physical layer addresses” (5-3).
Signal ID	The Signal ID field specifies the multiplexing structure of a transmission signal.
All Defects	Selecting the All Defects field requests information about all equipment and transmission defects.
Between	Selecting the Between field requests information about equipment or transmission defects that occurred between the dates and times that you specify.

Field name	Description
During the previous Day(s)	Selecting the During the previous Day(s) field requests information about equipment or transmission defects that occurred during the previous number of days that you specify. The values are 1–999.
During the previous Hour(s)	Selecting the During the previous Hour(s) field requests information about equipment or transmission defects that occurred during the previous number of hours that you specify. The values are 1–48.
During the previous Minute(s)	Selecting the During the previous Minute(s) field requests information about equipment or transmission defects that occurred during the previous number of minutes that you specify. The values are 1–120.

Related topic For general information about windows, see “About the main application window” (4-10).



Querying defects

- Procedure
- 1

Go to the Defects window at *Reports > Defects*.
- 2

Select the Port ID.
To query all ports, units, or subracks, select ALL for one or more Port ID fields.
- 3

Select the Signal ID if applicable.
To select a specific signal level, select a value other than ALL for each of the Signal ID fields.
- 4

Select one of the following fields:
 - All Defects
 - Between
 - During the previous Day(s)
 - During the previous Hour(s)
 - During the previous Minute(s)
- 5

Click Query.
- END OF STEPS



Defects query results

Illustration Use the following illustration only as an example of query results for the Defects window.

The screenshot shows a window titled "Reports - Defects - Query Results" with a menu bar (File, Edit, Help) and a status bar indicating "Query Completed 1999/03/01 12:45:07". The main area displays a table with the following data:

	Date of Defect	Time of Defect	Equipment ID	Signal ID	Condition	Severity	Category	SA Sta
1	1999/03/01	12:45:07	PSA-5-STN1-4-3	ADG#1-AU4-TUG3#2-TUG2#1-TU12#1	SYNCELTRF	PROMPT	TRANSMISSION	NSA
2	1999/03/01	13:45:07	PSA-6-STN1-3-3	ADG#1-AU4-TUG3#2-TUG2#1-TU12#1	SYNCESTRF	DEFERRED	EQUIPMENT	SA

At the bottom of the window are buttons for "Print...", "Close", and "Help".

Important! The data displayed on this screen may *not* be typical.

Results field descriptions

The following information appears in the Defects Query Results window. Click on a field name to see the field description.

Column	Description
Date of Defect	The Date of Defect column displays the date the system detected the defect.
Time of Defect	The Time of Defect column displays the time the system detected the defect.
Equipment ID	The Equipment ID column displays the physical location of the equipment on which the defect was detected. For a description of equipment addresses, see "About physical layer addresses" (5-3).
Signal ID	The Signal ID column displays the multiplexing structure of the transmission signal on which the defect was detected. For a description of the Signal ID options, see "About signal layer addresses" (5-4).
Condition	The Condition column displays the failure condition associated with the defect.
Severity	The Severity column displays the alarm severity associated with the defect as Info, Deferred, or Prompt.

Column	Description
Category	The Category column displays the defect category as Equipment or Transmission. For more information, see “Differences between transmission and equipment defects or failures” (6-3).
SA Status	The SA Status column displays the service-affecting status of the defect as Service Affecting or Non-Service Affecting.

Related topic For general information about windows, see “About the main application window” (4-10).





9 Equipment protection switching

Overview

Purpose “Equipment protection switching” contains the following information:

- General information about equipment protection switching
- Descriptions of the windows that are used to request equipment protection switching
- Step-by-step procedures for requesting equipment protection switching

Organisation “Equipment protection switching” is organised as follows:

- “Background information” (9-2)
- “MS Control window and procedures” (9-8)
- “Matrix Slice window and procedures” (9-19)
- “DTU window and procedures” (9-39)
- “STM1 1:8 window and procedures” (9-50)
- “MC Control window and procedures” (9-61)
- “Console screen procedures” (9-65)



Background information

Overview

Purpose This section contains background information about equipment protection switching.

Organisation This section is organised as follows:

- “Which window to use” (9-3)
- “Equipment protection switching terms” (9-4)
- “Protection switching concepts” (9-5)
- “Protection switching priorities” (9-7)



Which window to use

Protection switching table

Use the following table to determine which window to use when requesting a protection switch or querying the status of a protection group.

If the entity address is	Use the following window
MC-{1, 2}	MC Control for queries
	console terminal for protection switch requests
MS-3-SRC-GRP ¹	MS Control
MS-3-BSSU-{1-10} ²	Matrix Slice
PSA-{4-11, 4-19}-DTU-GRP	DTU
PSA-{4-11, 4-19}-STM1-{GRP1, GRP2}	STM1 1:8
PSA-{4-11, 4-19}-STM1-MSP{1, 3, 5, 7, 11, 13, 15, 17}-{1-4}	Protection Switch - Transmission
PSC-{4-11, 4-19}-STM4-MSP{1, 3, 5, 7}-{1-4}	
PSC-{4-11, 4-19}-STM16-MSP{1, 3, 5, 7}-1	

Notes:

1. Includes the SRC, STU, BSC, and both OLUs
2. Applies to both the BSSU and BSIU sides of a fibre



Equipment protection switching terms

- List of terms**
- Current request** A current request is the current state of the entity with regard to protection switching. A current request is either the result of a previous user-initiated protection switch request or the result of a system-initiated switch request that was made due to the condition of the software and hardware.
- Nonrevertive** Nonrevertive is a protection-switching operation type. When a protection group is nonrevertive, the protection entity will continue to operate as the active entity even after a failure clears on the working entity.
- Revertive** Revertive is a protection-switching operation type. When a protection group is revertive, the system will automatically switch service from the protection entity back to the working entity when a failure clears and the Wait-To-Restore time has elapsed.
- Wait-To-Restore (WTR) Time** The Wait-To-Restore (WTR) Time is the amount of time (in minutes) that the system waits, after a failure condition that caused a protection switch clears, before switching back to the previously-active equipment (matrix slice or STM-1 unit).



Protection switching concepts

Working and protection Working and protection are physical designations that are permanently associated with a hardware entity or set of hardware entities. A working entity is the hardware that normally provides service. A protection entity substitutes for a working entity as a result of a protection switching request.

Active and standby Active and standby are service designations that refer to the operational states of entities in a protection group. Either the working or protection entity may be active. An active entity is the hardware that is currently providing service. A standby entity is hardware that is not providing service, but may become active as the result of a protection switch.

Protection architecture The protection architecture determines how each piece of hardware is protected. Different pieces of hardware can have different protection architectures.

There are two general classes of protection architectures, M:N and N+M. The following table describes these architectures.

Symbol	Description
M	The number of sets of protection hardware
N	The number of sets of working hardware
:	The protection entity must have the provisioning information assigned to the working entity before the protection entity can become active.
+	The protection entity is already initialised with the provisioning information assigned to the working entity.

Protection arrangements The DACS system provides three types of protection arrangements.

Protection	Description
1+1	There is one protection unit (or group of units) for one working unit (or group of units).
1:8	There is one protection unit for a group of eight working units.

Protection	Description
2:8	The matrix and internal transmission paths are composed of ten sets of components. Each set of components is called a slice. Under normal circumstances, slices one through eight, the working slices, carry all the system traffic. Slices nine and ten provide protection. A protection slice can substitute for one of the working slices or for the other protection slice.

Operation types The following is a list of equipment protection and operation types on the DACS system.

Equipment protection	Operation type
Matrix slice	2:8 revertive
MS control	1+1 nonrevertive
DTU	1+1 nonrevertive
STM1-1:8	1:8 revertive
MC control	1+1 nonrevertive (when MC is duplicated)



Protection switching priorities

Priorities and protection switching requests

Whether the system will allow a protection-switching request often depends on the state of health of the active and the standby entities. The system evaluates several hardware and software states to determine the state of health of each entity. If the standby entity is found to be healthier than the active entity, a protection switch will occur.

When a protection-switching request is made, the system adds that request to other information the system considers when determining state of health. Furthermore, each protection-switching request has its own priority. By determining the state of health of both the active and the standby entities, and by evaluating the priorities of protection-switching requests, the system can determine whether one request takes precedence over another.

Priority states

The system will accept a protection-switching request only if that request has a sufficient priority. The current request is a result of either of the following:

- A previous user-initiated switch request
- A system-initiated switch request that resulted from the condition of the software and hardware



MS Control window and procedures

Overview

Purpose Use the MS Control window to query protection switch or unit status, or to request a protection switch for the Matrix/Synchronisation Control Complex (MS-3-SRC-GRP). Each working or protection MS Control entity consists of one SRC, one STU, one BSC, and two OLUs.

Window location *Protection > Equipment > MS Control*

Organisation This section is organised as follows:

- [“MS Control window description” \(9-9\)](#)
- [“Querying the current status of MS Control” \(9-11\)](#)
- [“MS Control query results” \(9-12\)](#)
- [“MS Control Current Req descriptions” \(9-14\)](#)
- [“MS Control Current Req list of priorities” \(9-16\)](#)
- [“MS Control unit condition descriptions” \(9-17\)](#)
- [“Requesting an MS Control protection switch” \(9-18\)](#)



MS Control window description

Illustration The following illustration shows the MS Control window.



MS Control field descriptions

The MS Control window has the following fields.

Field name	Description
Freeze	The Freeze field freezes the working and protection control complexes in their current active or standby state.
Clear Freeze	The Clear Freeze field clears a previously-requested freeze.
Force Switch to Working	The Force Switch to Working field forces service to the working control complex, regardless of whether the working control complex is in the active, standby, or failed current state. If the working control complex is already active, it remains active.
Force Switch to Protect	The Force Switch to Protect field forces service to the protection control complex, regardless of whether the protection control complex is in the active, standby, or failed current state. If the protection control complex is already active, it remains active.

Field name	Description
Clear Forced Switch	The Clear Forced Switch field clears a previously-requested forced switch.
Manual Switch to Working	The Manual Switch to Working field switches service to the working control complex if no higher priority request is active, and if no failure condition exists. If the working control complex is already active, it remains active.
Manual Switch to Protect	The Manual Switch to Protect field switches service to the protection control complex if no higher priority request is active, and if no failure condition exists. If the protection control complex is already active, it remains active.
Clear Manual Switch	The Clear Manual Switch field clears a previously-requested manual switch.

Related topics For more information, see any of the following topics:

- “About the main application window” (4-10)
- “Equipment protection switching terms” (9-4)
- “Protection switching concepts” (9-5)
- “Protection switching priorities” (9-7)



Querying the current status of MS Control

Procedure

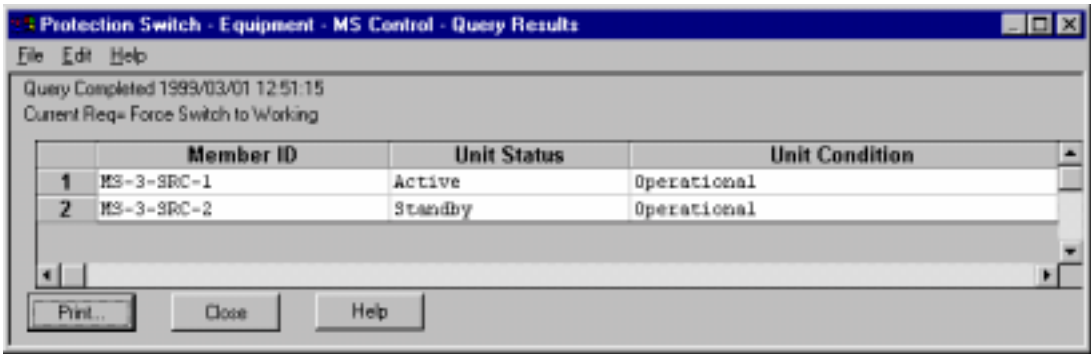
- 1** Go to the MS Control window at *Protection > Equipment > MS Control*.
 - 2** Click Query.
-

END OF STEPS



MS Control query results

Illustration Use the following illustration only as an example of query results from the MS Control window.



Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the table in the MS Control Query Results window.

Column	Description
Current Req	The Current Req displays the current request.
Member ID	The Member ID column displays the entity addresses for both the working and protection side SRCs.
Unit Status	The Unit Status column displays the current status of each member ID as one of the following: - Active - Standby For more information about unit status, see “Active and standby” (9-5).
Unit Condition	The Unit Condition column displays the current control complex condition as one of the following: - Fatal - Side Fail - Operational

Related topics For more information, see any of the following topics:

- “About the main application window” (4-10)
- “Equipment protection switching terms” (9-4)
- “MS Control Current Req descriptions” (9-14)

- “MS Control Current Req list of priorities” (9-16)
- “MS Control unit condition descriptions” (9-17)



MS Control Current Req descriptions

Current Req value descriptions The following current request information appears at the top of the MS Control Query Results window.

Current Req value	Description
Force Switch to Protect	A user-initiated switch forced the controllers to protection and locked them. Further switching of lower priority failure conditions is restricted. A forced switch will remain in effect until a user requests either a Clear Forced Switch or a Force Switch to Working, or until a higher priority condition, namely Fatal, occurs.
Force Switch to Working	A user-initiated switch forced the controllers to working and locked them. Further switching of lower priority failure conditions is restricted. A forced switch will remain in effect until one of the following occurs: • You request a Clear Forced Switch • You request a Force Switch to Protect • The system detects a Fatal condition
Freeze	A user-initiated freeze has locked the controllers in their current active or standby state.
Unit Fail Protect	The protection controller has one or more fail conditions on any of the units within the controller entity.
Unit Fail Working	The working controller has one or more fail conditions on any of the units within the controller entity.
Manual Switch to Protect	A user has initiated a switch of the unit to protection. A manual switch will remain in effect until one of the following occurs: • You request a Clear Manual Switch • You request an equal priority switch, such as another Manual Switch • You request a higher priority switch, such as Force Switch or Freeze • The system detects a fatal condition, such as Fatal or Side Fail

Current Req value	Description
Manual Switch to Working	A user has initiated a switch of the unit to working. A manual switch will remain in effect until one of the following occurs: • You request a Clear Manual Switch • You request an equal priority switch, such as another Manual Switch • You request a higher priority switch, such as Force Switch or Freeze • The system detects a fatal condition, such as Fatal or Side Fail
Do Not Revert	The protection unit is active, and there are no current protection requests.
No Request	There are no current protection requests.

Related topics For more information, see any of the following topics:

- “MS Control field descriptions” (9-9)
- “MS Control query results” (9-12)
- “MS Control Current Req list of priorities” (9-16)
- “MS Control unit condition descriptions” (9-17)



MS Control Current Req list of priorities

Current Req list of priorities

The following is a list of current request values displayed in the order of priority from highest to lowest. These values are displayed in the Current Req field at the top of the MS Control Query Results window.

1. Force Switch to Protect or Force Switch to Working
2. Freeze
3. Unit Fail Protect or Unit Fail Working
4. Manual Switch to Protect or Manual Switch to Working
5. Do Not Revert or No Request

Related topics

For more information, see any of the following topics:

- “Protection switching priorities” (9-7)
- “MS Control query results” (9-12)
- “MS Control Current Req descriptions” (9-14)
- “MS Control unit condition descriptions” (9-17)



MS Control unit condition descriptions

Unit condition value descriptions

The following is a list of possible unit condition values that appear in the MS Control Query Results window.

Value	Description
Fatal	The system has detected a fatal failure on either the active or the standby unit. This failure means that either the SRC unit or the BSC unit was removed or lost power. This situation usually results in a switch to standby, unless the standby unit also has a fatal failure.
Side Fail	Any of the controller units has one or more failures.
Operational	The controller units are fully operational.

Related topics

For more information, see any of the following topics:

- “MS Control query results” (9-12)
- “MS Control Current Req descriptions” (9-14)
- “MS Control Current Req list of priorities” (9-16)



Requesting an MS Control protection switch

Procedure

- 1 Go to the MS Control window at *Protection > Equipment > MS Control*.
-

- 2 Select the desired switch request.

Reference:

For a description of each switch request, see “MS Control window description” (9-9).

- 3 Click Apply.

Result:

If you attempt a forced switch to a faulted side, the system displays a confirmation message, giving you the chance to cancel the request. If there is a fatal condition on either side of the MS Control complex, the system denies a forced switch to the side with the fatal condition.

END OF STEPS



Matrix Slice window and procedures

Overview

Purpose Use the Matrix Slice window to query protection switch or unit status, or to request a protection switch for the matrix slice protection group. This protection group consists of ten sets of components. Each set of components is called a slice. Each slice consists of a BSSU and all the BSIUs connected to that BSSU. Requests are made on a per-matrix-slice basis.

Window location *Protection > Equipment > Matrix Slice*

Organisation This section is organised as follows:

- [“Matrix Slice window description” \(9-20\)](#)
- [“Querying the matrix slice” \(9-22\)](#)
- [“Matrix slice query results” \(9-23\)](#)
- [“Matrix slice Current Req descriptions” \(9-25\)](#)
- [“Matrix slice Current Req list of priorities” \(9-27\)](#)
- [“Matrix slice unit condition descriptions” \(9-28\)](#)
- [“Freezing the matrix slice” \(9-29\)](#)
- [“Forcing a switch to protection” \(9-31\)](#)
- [“Clearing a forced switch” \(9-32\)](#)
- [“Manually switching to protection” \(9-33\)](#)
- [“Clearing a manual switch” \(9-34\)](#)
- [“Locking service off of protection” \(9-35\)](#)
- [“Clearing a lock off” \(9-36\)](#)
- [“Locking service on to working” \(9-37\)](#)
- [“Clearing a lock on” \(9-38\)](#)



Matrix Slice window description

Illustration The following illustration shows the Matrix Slice window.



Matrix Slice field descriptions

The Matrix Slice window has the following fields.

Field name	Description
Freeze	The Freeze field freezes the working and protection slices in their current active/standby state.
Clear Freeze	The Clear Freeze field clears a previously-requested freeze.
Force Switch to Protect	The Force Switch to Protect field forces service to the desired protection slice. However, if the selected protection slice has a failure or degraded condition associated with it, the system will display a confirmation message to allow you to cancel the forced switch request or to continue with it. If the protection slice is already active, it remains active.
Clear Forced Switch	The Clear Forced Switch field clears a previously-requested forced switch.

Field name	Description
Manual Switch to Protect	The Manual Switch to Protect field switches service to the protection slice if no higher priority request is active, and if no failure condition exists. If the protection slice is already active, it remains active.
Clear Manual Switch	The Clear Manual Switch field clears a previously-requested manual switch.
Lock Service Off of Protect	The Lock Service Off of Protect field switches service back to working and prevents any future switches to the specified protection slice.
Clear Lock Off	The Clear Lock Off field clears a previously-requested lock off.
Lock Service On to Working	If the working slice is on protection, the Lock Service On to Working field will switch the slice back to working. The working slice will then be prevented from switching to protection.
Clear Lock On	The Clear Lock On field clears a previously-requested lock on.
Working Slice	The Working Slice field specifies which working slice (1–8) the protection switch request applies to.
Protect Slice	The Protect Slice field specifies which protection slice (9 or 10) the protection switch request applies to.

Related topics For more information, see any of the following topics:

- “About the main application window” (4-10)
- “Equipment protection switching terms” (9-4)
- “Protection switching concepts” (9-5)
- “Protection switching priorities” (9-7)



Querying the matrix slice

Procedure

- 1** Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.
-

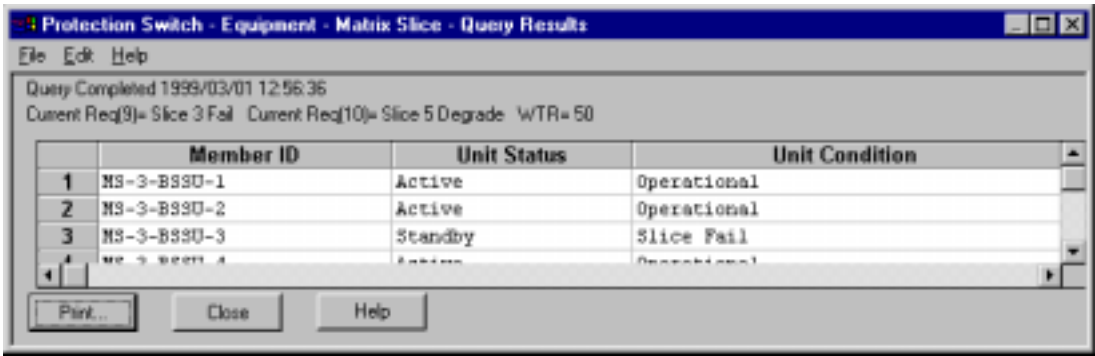
- 2** Click Query.

END OF STEPS



Matrix slice query results

Illustration Use the following illustration only as an example of query results from the Matrix Slice window.



Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the table in the Matrix Slice Query Results window.

Column	Description
Current Req	The Current Req displays the current request. Current Req(9) displays the current request status for slice 9 and Current Req(10) displays the current request status for slice 10. Slices 9 and 10 are the protection slices for the 2:8 matrix slice protection group.
WTR	The Wait-To-Restore (WTR) time value is displayed to the right of the Current Req information. The WTR value is in the range of 0–60 minutes. The default value is 5 minutes.
Member ID	The Member ID column displays the entity addresses of each BSSU in the format: MS-3-BSSU-{1–10}
Unit Status	The Unit Status column displays the current status as one of the following: - Active - Standby

Column	Description
Unit Condition	The Unit Condition column displays the unit condition for each member of the matrix slice protection group as one of the following: • Locked & Slice Fail • Locked & Slice Degrade • Locked & Operational • Slice Fail • Slice Degrade • Operational

Related topics For more information, see any of the following topics:

- “About the main application window” (4-10)
- “Equipment protection switching terms” (9-4)
- “Matrix slice Current Req descriptions” (9-25)
- “Matrix slice Current Req list of priorities” (9-27)
- “Matrix slice unit condition descriptions” (9-28)



Matrix slice Current Req descriptions

Current Req value descriptions

The following current request information appears at the top of the Matrix Slice Query Results window. Notice that there are two Current Req items shown — one for slice 9 and the other for slice 10. Slices 9 and 10 are the protection slices for the 2:8 matrix slice protection group.

Current Req value	Description
Lock Service Off of Protect	A user-initiated Lock Off of Protect switches a protected slice back to working and prevents any further use of the protection slice. A lock off of protection will remain in effect until a user requests a Clear Lock Off.
Force Switch Slice {1–8} to Protect	A user-initiated switch forced the slice to the designated protection slice. Further switching of lower priority failure conditions is restricted. A forced switch will remain in effect until a user requests a Clear Forced Switch, a Lock Off, or another Force Switch.
Freeze	A user-initiated request that freezes the working and protection slices in their current active/standby state. Further switching of lower priority failure conditions is restricted. A Freeze will remain in effect until a user requests a Clear Freeze, or a higher priority request such as a Lock Off, a Lock On, or a Force Switch.
Freeze Slice {1–8} On Protect	One or two working slices were on protection when a freeze request was accepted.
Slice {1–10} Fail	The matrix slice has a failure, or there is an empty slot.
Slice {1–10} Degrade	The matrix slice has been degraded.
Manual Switch Slice {1–8} to Protect	A user has initiated a manual switch of the slice to the designated protection slice. A manual switch will remain in effect until one of the following occurs: • You request a Clear Manual Switch • You request a higher priority switch • The system detects a failure or degrade condition

Current Req value	Description
Wait To Restore Slice {1–8}	The Wait-To-Restore (WTR) timer is active. When a slice has failed or has become degraded and then the condition clears, the slice remains on protection for the duration of the WTR time and then switches back to working. Any failure or user request overrides the WTR timer.
No Request	There are no current protection requests.

Related topics For more information, see any of the following topics:

- “Matrix Slice field descriptions” (9-20)
- “Matrix slice query results” (9-23)
- “Matrix slice Current Req list of priorities” (9-27)
- “Matrix slice unit condition descriptions” (9-28)



Matrix slice Current Req list of priorities

Current Req list of priorities

The following is a list of current request values displayed in the order of priority from highest to lowest. These values are displayed in the Current Req field at the top of the Matrix Slice Query Results window.

1. Lock Service Off of Protect
2. Force Switch Slice {1–8} to Protect
3. Freeze or Freeze Slice {1–8} On Protect
4. Slice {1–10} Fail
5. Slice {1–10} Degrade
6. Manual Switch Slice {1–8} to Protect
7. Wait To Restore Slice {1–8}
8. No Request

Related topics

For more information, see any of the following topics:

- “Protection switching priorities” (9-7)
- “Matrix slice query results” (9-23)
- “Matrix slice Current Req descriptions” (9-25)
- “Matrix slice unit condition descriptions” (9-28)



Matrix slice unit condition descriptions

Unit condition value descriptions

The following is a list of possible unit condition values that appear in the Matrix Slice Query Results window.

Value	Description
Locked & Slice Fail	Service is locked on the working slice, or is locked off the protection slice, and the matrix slice has a failure, or a unit has been removed.
Locked & Slice Degrade	Service is locked on the working slice, or is locked off the protection slice, and the matrix slice has been degraded.
Locked & Operational	Service is locked on the working slice, or is locked off the protection slice, and the matrix slice is fully operational.
Slice Fail	The matrix slice has a failure, or a unit has been removed.
Slice Degrade	The matrix slice has been degraded.
Operational	The slice is fully operational.

Related topics

For more information, see any of the following topics:

- “Matrix slice query results” (9-23)
- “Matrix slice Current Req descriptions” (9-25)
- “Matrix slice Current Req list of priorities” (9-27)



Freezing the matrix slice

Procedure

- 1 Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.
- 2 Select Freeze.
- 3 Click Apply.

END OF STEPS



Clearing a freeze of the matrix slice

- Procedure**
- 1

Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.
- 2

Select Clear Freeze.
- 3

Click Apply.
- END OF STEPS
- ☐

Forcing a switch to protection

Procedure

- 1** Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.

- 2** Select Force Switch to Protect.

- 3** Select the Working Slice ID of the working slice that you want to switch.

- 4** Select the Protect Slice ID of the protection slice to which you want service to switch.

- 5** Click Apply.

Result:

If you attempt a forced switch to a protection side where there is a failure or a degraded condition, the system displays a confirmation message giving you the chance to cancel the request.

END OF STEPS



Clearing a forced switch

Procedure

1

Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.

2

Select Clear Forced Switch.

3

Select the Protect Slice ID of the protection slice on which you want to clear the forced switch.

4

Click Apply.

END OF STEPS

Manually switching to protection

- Procedure
- 1

Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.
- 2

Select Manual Switch to Protect.
- 3

Select the Working Slice ID of the working slice that you want to switch.
- 4

Select the Protect Slice ID of the protection slice to which you want service to switch.
- 5

Click Apply.
- END OF STEPS



Clearing a manual switch

- Procedure
- 1

Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.
- 2

Select Clear Manual Switch.
- 3

Select the Protect Slice ID of the protection slice on which you want to clear the manual switch.
- 4

Click Apply.
- END OF STEPS



Locking service off of protection

Procedure

- 1** Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.

- 2** Select Lock Service Off of Protect.

- 3** Select the Protect Slice ID of the protection slice that you want locked off.

- 4** Click Apply.

END OF STEPS



Clearing a lock off

- Procedure
- 1

Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.
- 2

Select Clear Lock Off.
- 3

Select the Protect Slice ID of the protection slice on which you want to clear the lock off.
- 4

Click Apply.
- END OF STEPS



Locking service on to working

Procedure

- 1** Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.

- 2** Select Lock Service On to Working.

- 3** Select the Working Slice ID of the working slice that you want locked on.

- 4** Click Apply.

Result:

If you attempt to lock service onto a failed slice, the system displays a confirmation message, giving you the chance to cancel the request.

END OF STEPS



Clearing a lock on

Procedure

1

Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.

2

Select Clear Lock On.

3

Select the Working Slice ID of the working slice on which you want to clear the lock on.

4

Click Apply.

END OF STEPS

DTU window and procedures

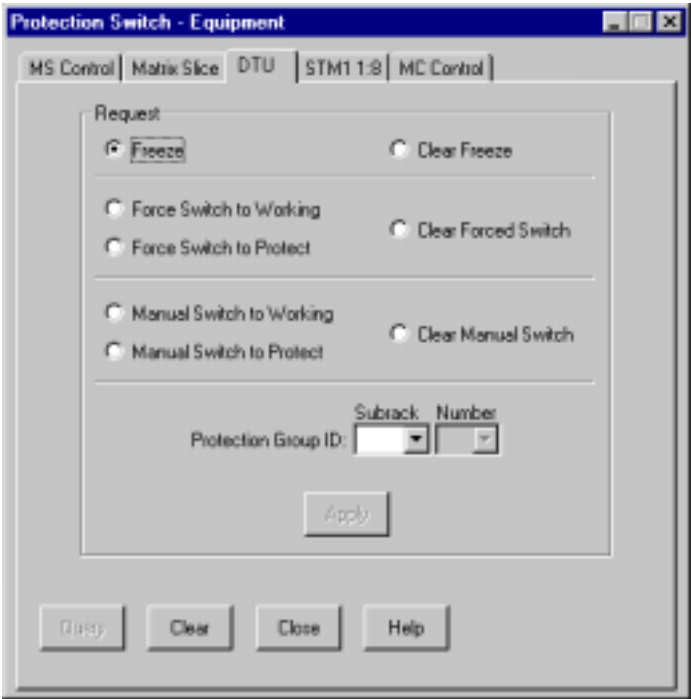
Overview

Purpose	Use the DTU window to query unit status or to request a protection switch for a DTU protection group.
Window location	<i>Protection > Equipment > DTU</i>
Organisation	This section is organised as follows: • <u>“DTU window description” (9-40)</u> • <u>“Querying a DTU protection group” (9-42)</u> • <u>“DTU query results” (9-43)</u> • <u>“DTU Current Req descriptions” (9-45)</u> • <u>“DTU Current Req list of priorities” (9-47)</u> • <u>“DTU unit condition descriptions” (9-48)</u> • <u>“Requesting a DTU protection group switch” (9-49)</u>



DTU window description

Illustration The following illustration shows the DTU window.



DTU field descriptions The DTU window has the following fields.

Field name	Description
Freeze	The Freeze field freezes the working and protection units in their current active/standby state.
Clear Freeze	The Clear Freeze field clears a previously-requested freeze.
Force Switch to Working	The Force Switch to Working field forces service to the working entity, regardless of whether the current state of the working entity is active, standby, or failed. If the working entity is already active, it remains active.
Force Switch to Protect	The Force Switch to Protect field forces service to the protection entity, regardless of whether the current state of the protection entity is active, standby, or failed. If the protection entity is already active, it remains active.
Clear Forced Switch	The Clear Forced Switch field clears a previously-requested forced switch.

Field name	Description
Manual Switch to Working	The Manual Switch to Working field switches service to the working unit if no higher priority request is active, and if no failure condition exists. If the working unit is already active, it remains active.
Manual Switch to Protect	The Manual Switch to Protect field switches service to the protection unit if no higher priority request is active, and if no failure condition exists. If the protection unit is already active, it remains active.
Clear Manual Switch	The Clear Manual Switch field clears a previously-requested manual switch.
Protection Group ID	The Protection Group ID field displays the address of the protection group. For a description of the Protection Group IDs, see “Equipment protection group addresses” (5-16).

Related topics For more information, see any of the following topics:

- “About the main application window” (4-10)
- “Equipment protection switching terms” (9-4)
- “Protection switching concepts” (9-5)
- “Protection switching priorities” (9-7)



Querying a DTU protection group

Procedure

- 1 Go to the DTU window at *Protection > Equipment > DTU*.
-

- 2 Select the Protection Group ID.

Reference:

For a description of the Protection Group IDs, see “Equipment protection group addresses” (5-16).

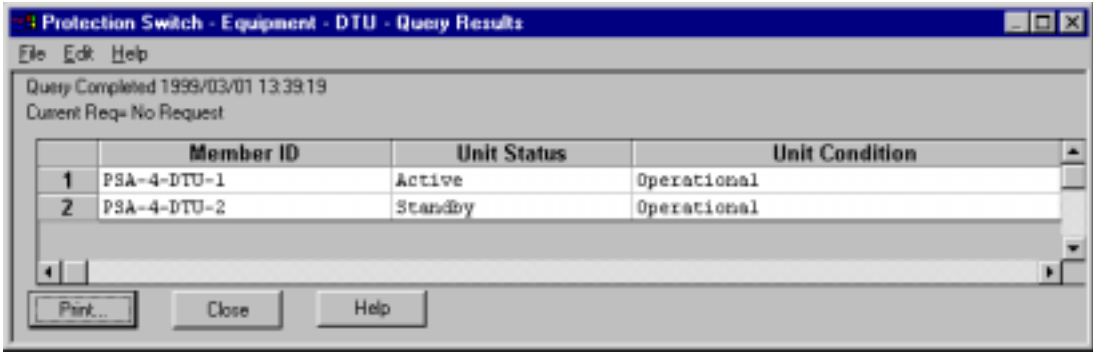
- 3 Click Query.

END OF STEPS



DTU query results

Illustration Use the following illustration only as an example of query results from the DTU window.



Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the table in the DTU Query Results window.

Column	Description
Current Req	The Current Req displays the current request.
Member ID	The Member ID column displays the entity addresses of the DTUs.
Unit Status	The Unit Status column displays the current status as one of the following: - Active - Standby For more information, see “Active and standby” (9-5).
Unit Condition	The Unit Condition column displays the unit condition field as one of the following: - Empty Slot - Under Test - Unit Fail - Operational

Related topics For more information, see any of the following topics:

- “About the main application window” (4-10)
- “Equipment protection switching terms” (9-4)
- “DTU Current Req descriptions” (9-45)

- “DTU Current Req list of priorities” (9-47)
- “DTU unit condition descriptions” (9-48)



DTU Current Req descriptions

Current Req value descriptions

The following current request information appears below the menu in the DTU Query Results window.

Current Req value	Description
Force Switch to Protect	A user has initiated a switch that has forced the unit to protection and locked it. Further switching of lower priority failure conditions is restricted. A forced switch will remain in effect until one of the following occurs: • You request a Clear Forced Switch • You request a Force Switch to Working • The system detects a higher priority condition, such as Empty Slot
Force Switch to Working	A user has initiated a switch that has forced the controllers to working and locked them. Further switching of lower priority failure conditions is restricted. A forced switch will remain in effect until one of the following occurs: • You request a Clear Forced Switch • You request a Force Switch to Protect • The system detects a higher priority condition, such as Empty Slot
Freeze	A user has initiated a freeze that has locked the units in their current active or standby state. Further switching of lower priority failure conditions is restricted. A freeze will remain in effect until one of the following occurs: • You request a Clear Manual Switch • You request a Manual Switch to Working • The system detects a higher priority condition, such as Empty Slot
Unit Fail Protect	The protection unit has a fail condition.
Unit Fail Working	The working unit has a fail condition.

Current Req value	Description
Manual Switch to Protect	A user has initiated a switch of the unit to protection. A manual switch will remain in effect until one of the following occurs: • You request a Clear Manual Switch • You request a Manual Switch to Working • You request a higher priority switch, such as Force Switch or Freeze • The system detects a fail condition
Manual Switch to Working	A user has initiated a switch of the unit to working. A manual switch will remain in effect until one of the following occurs: • You request a Clear Manual Switch • You request a Manual Switch to Protect • You request a higher priority switch, such as Force Switch or Freeze • The system detects a fail condition
Do Not Revert	The protection unit is active, and there are no current protection requests.
No Request	There are no current protection requests.

Related topics For more information, see any of the following topics:

- “DTU field descriptions” (9-40)
- “DTU query results” (9-43)
- “DTU Current Req list of priorities” (9-47)
- “DTU unit condition descriptions” (9-48)



DTU Current Req list of priorities

Current Req list of priorities

The following is a list of current request values displayed in the order of priority from highest to lowest. These values are displayed in the Current Req field at the top of the DTU Query Results window.

1. Force Switch to Protect or Force Switch to Working
2. Freeze
3. Unit Fail Protect or Unit Fail Working
4. Manual Switch to Protect or Manual Switch to Working
5. Do Not Revert or No Request

Related topics

For more information, see any of the following topics:

- “Protection switching priorities” (9-7)
- “DTU query results” (9-43)
- “DTU Current Req descriptions” (9-45)
- “DTU unit condition descriptions” (9-48)



DTU unit condition descriptions

Unit condition value descriptions

The following is a list of possible unit condition values that appear in the DTU Query Results window.

Value	Description
Empty Slot	The unit has been removed.
Under Test	There is a diagnostic test running on the unit.
Unit Fail	The unit has a failure.
Operational	The unit is fully operational.

Related topics

For more information, see any of the following topics:

- “DTU query results” (9-43)
- “DTU Current Req descriptions” (9-45)
- “DTU Current Req list of priorities” (9-47)



Requesting a DTU protection group switch

Procedure

- 1 Go to the DTU window at *Protection > Equipment > DTU*.
-

- 2 Select the desired switch request.

Reference:

For a description of each switch request, see “DTU window description” (9-40).

- 3 Select the Protection Group ID.

For a description of the Protection Group IDs, see “Equipment protection group addresses” (5-16).

- 4 Click Apply.

Result:

If you attempt a forced switch to a faulted side, the system displays a confirmation message, giving you the chance to cancel the request. If there is a Fatal (empty slot) condition associated with the DTU port, the system denies a forced switch to that DTU.

END OF STEPS



STM1 1:8 window and procedures

Overview

Purpose Use the STM1 1:8 window to query unit status and to request a protection switch for an STM-1 1:8 protection group.

Window location *Protection > Equipment > STM1 1:8*

Organisation This section is organised as follows:

- [“STM1 1:8 window description” \(9-51\)](#)
- [“Querying STM-1 1:8 protection groups” \(9-53\)](#)
- [“STM1 1:8 query results” \(9-54\)](#)
- [“STM1 1:8 Current Req descriptions” \(9-56\)](#)
- [“STM1 1:8 Current Req list of priorities” \(9-58\)](#)
- [“STM1 1:8 unit condition descriptions” \(9-59\)](#)
- [“Requesting an STM-1 1:8 protection switch” \(9-60\)](#)



STM1 1:8 window description

Illustration The following illustration shows the STM1 1:8 window.



STM1 1:8 field descriptions

The STM1 1:8 window has the following fields.

Field name	Description
Freeze	The Freeze field freezes the working and protection units in their current active/standby state.
Clear Freeze	The Clear Freeze field clears a previously-requested freeze.
Force Switch to Protect	The Force Switch to Protect field forces service to the protection entity, regardless of whether the protection entity is currently in the active, standby, or failed state. If the protection unit is already active, it remains active.
Clear Forced Switch	The Clear Forced Switch field clears a previously-requested forced switch.
Manual Switch to Protect	The Manual Switch to Protect field switches service to the protection unit if no higher priority request is active, and if no failure condition exists. If the protection unit is already active, it remains active.

Field name	Description
Clear Manual Switch	The Clear Manual Switch field clears a previously-requested manual switch.
Lock Service Off of Protect	The Lock Service Off of Protect field switches service back to working and prevents any future switches to protection.
Clear Lock Off	The Clear Lock Off field clears a previously-requested lock off.
Lock Service On to Working	The Lock Service On to Working field prevents a switch of a working unit to protection. If the working unit is already on protection, the system will switch it back to working.
Clear Lock On	The Clear Lock On field clears a previously-requested lock on.
Protection Group ID	The Protection Group ID field displays the address of the protection group. For a description of the Protection Group IDs, see “Equipment protection group addresses” (5-16).

Related topics For more information, see any of the following topics:

- “About the main application window” (4-10)
- “Equipment protection switching terms” (9-4)
- “Protection switching concepts” (9-5)
- “Protection switching priorities” (9-7)



Querying STM-1 1:8 protection groups

Procedure

- 1 Go to the STM1 1:8 window at *Protection > Equipment > STM1 1:8*.
-

- 2 Select the Protection Group ID.

Reference:

For a description of the Protection Group IDs, see “Equipment protection group addresses” (5-16).

- 3 Click Query.

END OF STEPS



STM1 1:8 query results

Illustration Use the following illustration only as an example of query results from the STM1 1:8 window.



Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the table in the STM1 1:8 Query Results window.

Column	Description
Current Req	The Current Req displays the current request.
WTR	The Wait-To-Restore (WTR) time value displays to the right of the Current Req information. The WTR value will be in the range of 0–60 minutes. The default value is 5 minutes.
Member ID	The Member ID column displays the entity address of each STM-1 unit in the group.
Unit Status	The Unit Status column displays the current status as one of the following: - Active - Standby For more information, see “Active and standby” (9-5).

Column	Description
Unit Condition	The Unit Condition column displays the current unit condition. The following unit conditions are listed in the order of priority: 1. Deleted Unit 2. Locked & IU Not Available 3. Locked & Empty Slot 4. Locked & Under Test 5. Locked & Unit Fail 6. Locked & Operational 7. Transmission Protected 8. IU Not Available 9. Empty Slot 10. Under Test 11. Unit Fail 12. Operational

Related topics For more information, see any of the following topics:

- “About the main application window” (4-10)
- “Equipment protection switching terms” (9-4)
- “Protection switching priorities” (9-7)
- “STM1 1:8 Current Req descriptions” (9-56)
- “STM1 1:8 Current Req list of priorities” (9-58)
- “STM1 1:8 unit condition descriptions” (9-59)



STM1 1:8 Current Req descriptions

Current Req value descriptions

The following current request information appears at the top of the STM1 1:8 Query Results window.

Current Req value	Description
Protection Not Available	The protection unit for an STM-1 1:8 protection group has been removed. This condition completely disables any protection capabilities for this group. A Protection Not Available condition will remain in effect until a protection unit is installed.
Lock Service Off of Protect	Service was switched back to working. The system will prevent any future switches to the protection unit until you execute a Clear Lock Off request.
Force Switch Unit {1–8, 11–18} to Protect	A user has initiated a switch that forced the unit to protection and locked it. Further switching of lower priority failure conditions is restricted. A forced switch will remain in effect until one of the following occurs: - You request a Clear Forced Switch - You request a Forced Switch - You request a Lock Off - The system detects a higher priority condition
Freeze	A user has initiated a freeze of the working and protection units in their current active/standby state. Further switching of lower priority failure conditions is restricted. A freeze will remain in effect until you request a Clear Freeze, Lock Off, Lock On, or Force Switch.
Freeze Unit {1–8, 11–18} on Protect	A unit was already on protection when the freeze request was accepted.
Unit {1–9, 11–19} Fail	The unit has a failure, or the unit has been removed. If the unit has been removed from slot 9 or slot 19, the Current Req value will be Protection Not Available.

Current Req value	Description
Manual Switch Unit {1–8, 11–18} to Protect	A user has initiated a manual switch of the unit to the designated protection unit. A manual switch will remain in effect until any other user-initiated request is made or until a failure condition occurs.
Wait To Restore Unit {1–8, 11–18}	The Wait-To-Restore (WTR) timer is active. When a unit has failed or has become degraded and then the condition clears, the unit remains on protection for the duration of the WTR time and then switches back to working. Any failure or user request overrides the WTR timer.
No Request	There are no current protection requests.

Related topics For more information, see any of the following topics:

- “Equipment protection switching terms” (9-4)
- “STM1 1:8 field descriptions” (9-51)
- “STM1 1:8 query results” (9-54)
- “STM1 1:8 Current Req list of priorities” (9-58)
- “STM1 1:8 unit condition descriptions” (9-59)



STM1 1:8 Current Req list of priorities

Current Req list of priorities

The following is a list of current request values displayed in the order of priority from highest to lowest. These values are displayed in the Current Req field at the top of the STM1 1:8 Query Results window.

1. Protection Not Available
2. Lock Service Off of Protect
3. Force Switch Unit {1–8, 11–18} to Protect
4. Freeze or Freeze Unit {1–8, 11–18} on Protect
5. Unit {1–9, 11–19} Fail
6. Manual Switch Unit {1–8, 11–18} to Protect
7. Wait To Restore Unit {1–8, 11–18}
8. No Request

Related topics

For more information, see any of the following topics:

- “Protection switching priorities” (9-7)
- “STM1 1:8 Current Req descriptions” (9-56)
- “STM1 1:8 query results” (9-54)
- “STM1 1:8 unit condition descriptions” (9-59)



STM1 1:8 unit condition descriptions

Unit condition value descriptions

The following is a list of possible unit condition values that appear in the STM1 1:8 Query Results window.

Value	Description
Deleted Unit	The unit has been deleted or has never been booted. This unit cannot be protected.
Locked & IU Not Available	The working unit is locked on and the Interface Unit (IU) is missing, is an optical IU, or is not available. The associated unit cannot be protected.
Locked & Empty Slot	The working unit is locked on, or the protection unit is locked off, and the unit has been removed.
Locked & Under Test	The working unit is locked on, or the protection unit is locked off, and a diagnostic is running on the unit.
Locked & Unit Fail	The working unit is locked on, or the protection unit is locked off, and the unit has a failure.
Locked & Operational	The working unit is locked on, or the protect unit is locked off, and the unit is fully operational.
Transmission Protected	The unit has at least one Multiplex Section Protection (MSP) group provisioned.
IU Not Available	The Interface Unit (IU) is missing, is an optical IU, or is not available. The associated unit cannot be protected.
Empty Slot	The unit has been removed.
Under Test	A diagnostic test is running on the unit.
Unit Fail	The unit has a failure.
Operational	The unit is fully operational.

Related topics

For more information, see any of the following topics:

- “STM1 1:8 Current Req descriptions” (9-56)
- “STM1 1:8 query results” (9-54)
- “STM1 1:8 Current Req list of priorities” (9-58)



Requesting an STM-1 1:8 protection switch

Procedure

- 1 Go to the STM1 1:8 window at *Protection > Equipment > STM1 1:8*.
-

- 2 Select the desired switch request.

Reference:

For a description of each switch request, see “STM1 1:8 window description” (9-51).

- 3 Select the Protection Group ID.
-

- 4 Click Apply.

Result:

If you attempt a Force Switch to Protect to a failed unit, the system displays a confirmation message, giving you the chance to cancel the request.

END OF STEPS



MC Control window and procedures

Overview

Purpose Use the MC Control window to query unit status for the Main Controller.

Window location *Protection > Equipment > MC Control*

Organisation This section is organised as follows:

- “MC Control window description” (9-62)
- “Querying the MC from the user interface” (9-63)
- “MC Control query results” (9-64)



MC Control window description

MC Control field descriptions The MC Control window has no fields. This window can only be used to query unit status for the Main Controller.

Related topic For more information, see “About the main application window” (4-10).



Querying the MC from the user interface

Procedure

- 1** Go to the MC Control window at *Protection > Equipment > MC Control*.
-

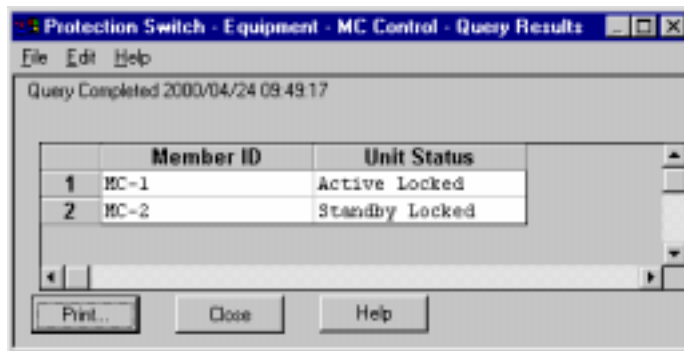
- 2** Click Query.

END OF STEPS



MC Control query results

Illustration Use the following illustration only as an example of query results from the MC Control window.



Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the table in the MC Control Query Results window.

Column	Description
Member ID	The Member ID column displays the entity address of the Main Controller.
Unit Status	The Unit Status column displays the current status of each member ID as one of the following: • Active • Standby • Active Locked • Standby Locked For more information, see “Active and standby” (9-5).

Related topics For more information, see any of the following topics:

- “About the main application window” (4-10)
- “Equipment protection switching terms” (9-4)



Console screen procedures

Overview

- Purpose** You must use the console screen to switch the Main Controller (MC), remove the MPU from service, and restore the MPU to service.
- Organisation** This section is organised as follows:
- [“MC Control window description” \(9-62\)](#)
 - [“Querying the MC from the user interface” \(9-63\)](#)
 - [“MC Control query results” \(9-64\)](#)
- Related topics** The following procedures are also performed from the console terminal:
- [“Removing the MPU on a duplicated MC configuration” \(11-18\)](#)
 - [“Restoring the DB on an MPU with a duplicated MC configuration” \(11-23\)](#)
 - [“Restoring the DB on an MPU with a single MC configuration” \(11-29\)](#)



MC duplication terms

- List of terms**
- Active and standby** These terms refer to the operational state of a Main Controller (MC). The active MC is the one that is currently providing service; the standby MC substitutes for the active MC if necessary.
- Duplex** A duplex MC configuration means that the MCs are operating in a database replicating mode. This means that changes to the system database are being copied from the active MC to the standby MC.
- Lock** A lock switch request is a manual request that prevents the MCs from switching from active to standby and vice versa.
- Simplex** A simplex MC configuration means that the MCs are operating in a non database replicating mode. This means that changes to the system database are not being copied from the active MC to the standby MC. Also, no alarms are generated for the standby MC. Simplex mode is used only for software upgrades. Autonomous switching can still occur while the system is in simplex mode.
- Unlock** An unlock switch request removes a previously-requested lock on the MCs.
- Working and protection** These terms refer to the physical designation of the MCs. MC-1 is designated as the working entity, while MC-2 is designated as the protection entity. If the status of the MC-1 changes from active to standby, MC-1 still retains its designation as the working entity. The working entity is the preferred active entity.



Console terminal connections

What is a console terminal?

Use the console terminal to perform DACS functions that you cannot perform from the user interface. These functions include protection switching the Main Controller (MC) in a duplicated configuration, and performing hardware and software upgrades.

Types of console terminals

You can use a VT100-compatible terminal or a PC with Telnet application software.

Connections

Connect the console terminal to one of the following:

- WS1 on the User Panel for the working MC (MC-1)
- WS2 on the User Panel for the protection MC (MC-2)



Getting to the MC Duplication Functions screen

Purpose You will need to perform the majority of Main Controller (MC) functions from the MC Duplication Functions screen, not from the DACS user interface windows. This procedure describes how to get to the MC Duplication Functions screen. You can use this screen to perform queries, request protection switches, and define the identity of a controller. You can also perform a query from the user interface at *Protection > Equipment > MC Control*.

Procedure

- 1 Make sure you have a console terminal connection to the appropriate MC subrack.

Result:

After you connect to the MC, the following screen appears:

```
LynxOS (w001)
user name:
```

One of the following displays after LynxOS:

- If the terminal is connected to the working MC, w001 displays.
 - If the terminal is connected to the protection MC, w002 displays.
-

- 2 At the prompt, type `admin` and then press **ENTER**

Result:

```
DACS                               System Administration

                                Main Menu

1 - EXLAN IP Assignment
2 - Database Backup
3 - Special MO functions
4 - Reboot the MC
5 - Reboot the System
6 - Change admin Password
7 - MC Duplication Functions
? - Help
q - Quit

Enter choice:
```


- Result:**

Enter special MC Duplication password and hit <return>

- Result:**

```

DACs                                     System Administration
                                     MC Duplication Functions

1 - Query Duplication Status
2 - Switch MC Controller
3 - Change MC Simplex/Duplex
? - Help
p - Return to Main menu

Enter choice:

```

Reference:

If you do not know the password, call your Lucent Technologies account representative, or technical support.

END OF STEPS



Querying the MC from the console terminal

Purpose This procedure describes how to query the status of the active and standby Main Controllers (MCs) from a console terminal. You may prefer to perform queries from the user interface. For more information about how to perform a query from the user interface, see “Querying the MC from the user interface” (9-63).

Procedure

- 1 Go to the MC Duplication Functions screen.

Reference:

For more information, see “Getting to the MC Duplication Functions screen” (9-68).

- 2 At the prompt, press **1** (Query Duplication Status), and then press **ENTER**

Example:

```
This Controller's ID is working
This Controller's Status is active
This Controller's Lock is locked
This Controller's Mode is duplex
```

END OF STEPS



Requesting an MC protection switch

Purpose This procedure describes how to request the following protection switches of the Main Controllers (MCs):

- From active to standby, or from standby to active
- From locked to unlocked, or from unlocked to locked

Important! Executing the lock and unlock functions from one MC affects both the active and standby MCs.

Procedure

- 1 Go to the MC Duplication Functions screen.

Reference:

For more information, see “Getting to the MC Duplication Functions screen” (9-68).

- 2 Query the current protection status of the MC.

Reference: For more information, see one of the following:

- “Querying the MC from the console terminal” (9-70)
 - “Querying the MC from the user interface” (9-63)
-

- 3 At the prompt, press **2** (Switch MC Controller), and then press **ENTER**

Result:

```
DACS                               System Administration
                                MC Controller Switch

Set this Controller's State to
1 - Active
2 - Standby
3 - Lock
4 - Unlock
? - Help
p - Return to previous menu

Enter choice:
```

- 4 At the prompt, press the appropriate number, and then press **ENTER**

Result:

It may take several minutes for the newly-active MC to become operational, and before a query will reflect the current protection status.

END OF STEPS





10 MSP and SNCP switching

Overview

- Purpose** “MSP and SNCP switching” contains the following information:
- General information about Multiplex Section Protection (MSP) and Sub-Network Connection Protection (SNCP) switching
 - Descriptions of the windows that are used to request MSP or SNCP switching
 - Step-by-step procedures for requesting MSP or SNCP switching

- Organisation** “Transmission protection switching” is organised as follows:
- “Background information” (10-2)
 - “ITU and ANSI MSP current requests, priorities, and unit conditions” (10-6)
 - “NTT MSP current requests, priorities, and unit conditions” (10-12)
 - “MSP transmission window and procedures” (10-24)
 - “SNCP current requests, priorities, and unit conditions” (10-32)
 - “SNCP transmission window and procedures” (10-36)



Background information

Overview

Purpose This section contains background information about MSP and SNCP switching.

Organisation This section is organised as follows:

- “Switch request terms” (10-3)
- “MSP K byte mismatch state designations” (10-5)



Switch request terms

- List of terms**
- Current request** A current request is the current state of the entity with regard to protection switching. A current request is either the result of a previous user-initiated protection switch request or the result of a system-initiated switch request that was made due to the condition of the software and hardware.
- Far-end request (MSP only)** A far-end request is a remote protection-switching request of the Multiplex Section Protection (MSP) line.
- K bytes (MSP only)** K bytes are Automatic Protection Switching (APS) bytes that are used by the Multiplex Section Protection (MSP) functions at the ends of a multiplex section in making requests for, and giving acknowledgements of, protection-switching actions.
- Line condition (MSP only)** The line condition is the current state of health of a working or a protection line.
- Near-end request (MSP only)** A near-end request is a local protection-switching request of the Multiplex Section Protection (MSP) line.
- Nonrevertive** Nonrevertive is a protection-switching operation type. When a protection group is nonrevertive, the protection entity will continue to operate as the active entity even after a failure clears on the working entity.
- Line restore time (NTT MSP only)** Line restore time is the number of minutes that the system waits, after a failure condition that caused a protection switch clears, before switching to the line that is not carrying service (the line where the fault cleared). Line restore time applies only to NTT MSP.
- Revertive** Revertive is a protection-switching operation type. When a protection group is revertive, the system will automatically switch service from the protection entity back to the working entity when a failure clears and the Wait-To-Restore time has elapsed.
- Secondary line (NTT MSP only)** The secondary line is the line in an NTT MSP arrangement that provides service when there is an active protection request.

The secondary line is active or standby depending on the following conditions:

- If the current request state is No Request or Do Not Revert, the secondary line is the standby line.
- If the current request state is something other than No Request or Do Not Revert, the secondary line is the active line.

Signal Degrade A Signal Degrade means that the bit error rate of the multiplex section has exceeded the provisioned threshold for the provisioned number of seconds.

Trail Signal Fail Trail Signal Fail is a protection-switching condition that means that the system detected Multiplex Section-Alarm Indication Signal (MS-AIS), Loss of Frame (LOF), or Loss of Signal (LOS) on a line.

WTR Time The Wait-To-Restore (WTR) Time is the amount of time (in minutes) that the system waits, after a failure condition that caused a protection switch clears, before switching back to the previously-active equipment (matrix slice or STM-1 unit).

□

MSP K byte mismatch state designations

**K byte information
appended to ITU current
request states**

In some situations, ITU current requests can have additional K byte information (in the form *K1, *K2, or *K1 *K2) included as part of the request state.

The following are the possible values:

- *K1
The far-end system is requesting a different channel than the near-end system in the K1 byte, but the channel requested in the sent K1 byte is acknowledged in the received K2 byte.
- *K2
The far-end system is requesting the same channel as the near-end system in the K1 byte, but the requested channel is not yet acknowledged in the received K2 byte.
- *K1 *K2
Neither the received K1 channel nor the received K2 channel match the requested K1 channel.

Related topic

For a better understanding of K bytes, refer to ITU-T Recommendation G.841.



ITU and ANSI MSP current requests, priorities, and unit conditions

Overview

Purpose This section contains the ITU and ANSI MSP switching current requests, priorities, and unit condition information.

Organisation This section is organised as follows:

- “ITU and ANSI MSP Current Req values” (10-7)
- “ITU and ANSI MSP Current Req priorities” (10-10)
- “ITU and ANSI MSP unit condition values” (10-11)



ITU and ANSI MSP Current Req values

ITU and ANSI MSP Current Req value descriptions

The following Current Req information appears at the top of the Protection Switch - Transmission Query Results window.

Current Req value	Description
Do Not Revert	The protection line is the active line, and no forced switch condition, lockout condition, or protection line faults exist.
Do Not Revert Remote	The active line at the far-end system is the protection line. No forced switch condition, lockout condition, or protection line fault exists.
Force Switch to Protect	A user initiated a switch that forced the line to protection, and the near-end system is still transmitting K bytes indicating Force Switch to Protect. The protection line is the active line.
Force Switch to Protect Remote	A user initiated a switch on the far-end system that forced the line to protection, and the near-end system has responded. The protection line is the active line.
Force Switch to Working	A user initiated a switch that forced the line to working, and the near-end system is still transmitting K bytes indicating Force Switch to Working. The working line is the active line.
Force Switch to Working Remote	A user initiated a forced switch to working from the far-end system, and the near-end system has responded. The working line is the active line.
Lockout	A user initiated a lockout request from the near-end system when the previous request was No Request. The system will ignore line conditions and far-end system requests while Lockout is active. If you execute a Clear Switch Request, the Current Req on the near-end system will return to No Request.
Lockout Remote	A user manually switched the line to working, and the near-end system is still transmitting K bytes indicating Force Switch to Working.
Manual Switch to Protect	A user manually switched the line to protection, and the near-end system is still transmitting K bytes indicating Force Switch to Protect. The protection line is the active line.

Current Req value	Description
Manual Switch to Protect Remote	A user manually switched the line to protection from the far-end system, and the near-end system has responded. The protection line is the active line.
Manual Switch to Working	A user manually switched the line to working, and the near-end system is still transmitting K bytes indicating Force Switch to Working. The working line is the active line.
Manual Switch to Working Remote	A user manually switched the line to working from the far-end system, and the near-end system has responded. The working line is the active line.
No Request	There are no current protection requests.
Signal Degrade Protect	The system detected a signal degrade condition on the protection line. The signal degrade condition was transmitted by the near-end system and acknowledged by the far-end system. The near-end system continues to send K bytes indicating signal degrade. The working line is the active line.
Signal Degrade Protect Remote	The far-end system has requested a switch to the protection line due to a detected signal degrade on the protection line, and the near-end system has responded. The working line is the active line.
Signal Degrade Working	The system detected a signal degrade condition on the working line. The signal degrade condition was transmitted by the near-end system and acknowledged by the far-end system. The near-end system continues to send K bytes indicating signal degrade. The protection line is the active line.
Signal Degrade Working Remote	The far-end system has requested a switch to the protection line due to a detected signal degrade on the working line, and the near-end system has responded. The protection line is the active line.
Trail Signal Fail Protect	The near-end system has detected a trail signal fail on the protection line, and the far-end system has acknowledged it. The near-end system continues to send K bytes indicating trail signal fail. The working line is the active line.
Trail Signal Fail Protect Remote	The far-end system has requested a switch to the protection line due to a detected trail signal fail on the protection line, and the near-end system has responded. The working line is the active line.

Current Req value	Description
Trail Signal Fail Working	The system detected a trail signal fail on the working line. The trail signal fail was transmitted by the near-end system and acknowledged by the far-end system. The near-end system continues to send K bytes indicating trail signal fail. The protection line is the active line.
Trail Signal Fail Working Remote	The far-end system has requested a switch to the protection line due to a detected trail signal fail on the working line, and the near-end system has responded. The protection line is the active line.
Wait To Restore Protect	A line condition has cleared on the protection line, and the Wait-To-Restore timer is running. The working line is the active line.
Wait To Restore Protect Remote	A Wait-To-Restore for the protection line was initiated by the far-end system. The far-end system has signalled the starting of its WTR timer. The working line is the active line.
Wait To Restore Working	A line condition has cleared on the working line, and the WTR timer is running. The protection line is the active line.
Wait To Restore Working Remote	A Wait-To-Restore for the working line was initiated by the far-end system. The far-end system has signalled the starting of its WTR timer. The protection line is the active line.



ITU and ANSI MSP Current Req priorities

List of priorities The following list displays the ITU and ANSI MSP current request values in descending order of priority.

1. Lockout
2. Lockout Remote
3. Force Switch to Working
4. Force Switch to Working Remote
5. Force Switch to Protect
6. Force Switch to Protect Remote
7. Trail Signal Fail Working
8. Trail Signal Fail Working Remote
9. Trail Signal Fail Protect
10. Trail Signal Fail Protect Remote
11. Signal Degrade Working
12. Signal Degrade Working Remote
13. Signal Degrade Protect
14. Signal Degrade Protect Remote
15. Manual Switch to Working
16. Manual Switch to Working Remote
17. Manual Switch to Protect
18. Manual Switch to Protect Remote
19. Wait To Restore Working
20. Wait To Restore Working Remote
21. Wait To Restore Protect
22. Wait To Restore Protect Remote
23. Do Not Revert
24. Do Not Revert Remote
25. No Request

Related topic For a definition of priorities, see “Protection switching priorities” (9-7).



ITU and ANSI MSP unit condition values

Unit condition value
descriptions

The following is a list of possible ITU and ANSI MSP unit condition values that appear in the Protection Switch - Transmission Query Results window.

Value	Description
Empty Slot	The unit has been removed.
Line Clear	The unit is fully operational.
Signal Degrade	The bit error rate of the multiplex section has exceeded the provisioned threshold for the provisioned number of seconds.
Trail Signal Fail	Failure of the transmission signal (for example: LOS, or AIS) or unit, or the unit has been removed.
Unit Fail	The unit has a failure.

NTT MSP current requests, priorities, and unit conditions

Overview

Purpose This section contains the NTT MSP switching current requests, priorities, and unit condition information.

Organisation This section is organised as follows:

- “NTT MSP Current Req values” (10-13)
- “NTT MSP Current Req priorities” (10-21)
- “NTT MSP unit condition values” (10-23)



NTT MSP Current Req values

NTT MSP Current Req value descriptions

The following Current Req (current request) information appears at the top of the table in the Protection Switch - Transmission Query Results window.

Current Req value	Description
Do Not Revert	The protection line is the active line, and no forced switch condition, lockout condition, or protection line faults exist.
Force Switch to Protect	A user initiated a switch that forced the line to protection, and the near-end system is still transmitting K bytes indicating Force Switch to Protect. The protection line is the active line.
Force Switch to Protect Remote	A user initiated a switch on the far-end system that forced the line to protection, and the near-end system has responded. The protection line is the active line.
Force Switch to Protect Request	A user initiated a request from the near-end system that forced the protection line to active, but the far-end system has not yet responded. The near-end system will return to the previous request after one second if this request is not acknowledged by the far-end system. The working line is still the active line.
Force Switch to Working	A user initiated a switch that forced the line to working, and the near-end system is still transmitting K bytes indicating Force Switch to Working. The working line is the active line.
Force Switch to Working Remote	A user initiated a forced switch to working from the far-end system, and the near-end system has responded. The working line is the active line.
Force Switch to Working Request	A user initiated a request from the near-end system to force the working line active, but the far-end system has not yet responded. The near-end system will return to the previous request after one second if this request is not acknowledged by the far-end system. The protection line is still the active line.

Current Req value	Description
Lockout Do Not Revert	A user initiated a lockout request from the near-end system when the previous request was Do Not Revert. The system will ignore line conditions and far-end system requests while Lockout Do Not Revert is active. The protection line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Do Not Revert.
Lockout Force Switch Protect	A user initiated a lockout request from the near-end system when the previous request was Force Switch to Protect. The system will ignore line conditions and far-end requests while Lockout Force Switch Protect is active. The protection line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Force Switch to Protect.
Lockout Force Switch Protect Remote	A user initiated a lockout request from the near-end system when the previous request was Force Switch to Protect Remote. The system will ignore line conditions and far-end requests while Lockout Force Switch Protect Remote is active. The protection line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Force Switch to Protect Remote.
Lockout Force Switch Working	A user initiated a lockout request from the near-end system when the previous request was Force Switch to Working. The system will ignore line conditions and far-end requests while Lockout Force Switch Working is active. The working line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Force Switch to Working.

Current Req value	Description
Lockout Force Switch Working Remote	A user initiated a lockout request from the near-end system when the previous request was Force Switch to Working Remote. The system will ignore line conditions and far-end requests while Lockout Force Switch Working Remote is active. The working line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Force Switch to Working Remote.
Lockout No Request	A user initiated a lockout request from the near-end system when the previous request was No Request. The system will ignore line conditions and far-end requests while Lockout No Request is active. The working line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to No Request.
Lockout Signal Degrade Protect	A user initiated a lockout request from the near-end system when the previous request was Signal Degrade Protect. The system will ignore line conditions and far-end requests while Lockout Signal Degrade Protect is active. The working line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Signal Degrade Protect.
Lockout Signal Degrade Protect Remote	A user initiated a lockout request from the near-end system when the previous request was Signal Degrade Protect Remote. The system will ignore line conditions and far-end requests while Lockout Signal Degrade Protect Remote is active. The working line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Signal Degrade Protect Remote.

Current Req value	Description
Lockout Signal Degrade Working	A user initiated a lockout request from the near-end system when the previous request was Signal Degrade Working. The system will ignore line conditions and far-end requests while Lockout Signal Degrade Working is active. The protection line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Signal Degrade Working.
Lockout Signal Degrade Working Remote	A user initiated a lockout request from the near-end system when the previous request was Signal Degrade Working Remote. The system will ignore line conditions and far-end requests while Lockout Signal Degrade Working Remote is active. The protection line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Signal Degrade Working Remote.
Lockout Trail Signal Fail Working	A user initiated a lockout request from the near-end system when the previous request was Trail Signal Fail Working. The system will ignore line conditions and far-end requests while Lockout Trail Signal Fail Working is active. The protection line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Trail Signal Fail Working.
Lockout Trail Signal Fail Working Remote	A user initiated a lockout request from the near-end system when the previous request was Trail Signal Fail Working Remote. The system will ignore line conditions and far-end requests while Lockout Trail Signal Fail Working Remote is active. The protection line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Trail Signal Fail Working Remote.

Current Req value	Description
Lockout Trail Signal Fail Protect	A user initiated a lockout request from the near-end system when the previous request was Trail Signal Fail Protect. The system will ignore line conditions and far-end requests while Lockout Trail Signal Fail Protect is active. The working line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Trail Signal Fail Protect.
Lockout Trail Signal Fail Protect Remote	A user initiated a lockout request from the near-end system when the previous request was Trail Signal Fail Protect Remote. The system will ignore line conditions and far-end requests while Lockout Trail Signal Fail Protect Remote is active. The working line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Trail Signal Fail Protect Remote.
Lockout Wait To Restore Protect	A user initiated a lockout request from the near-end system when the previous request was Wait To Restore Protect. The system will ignore line conditions and far-end requests while Lockout Wait To Restore Protect is active. The working line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Wait To Restore Protect, and the system will restart the Wait-To-Restore timer with its full time-out value.
Lockout Wait To Restore Protect Remote	A user initiated a lockout request from the near-end system when the previous request was Wait To Restore Protect Remote. The system will ignore line conditions and far-end requests while Lockout Wait To Restore Protect Remote is active. The working line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Wait To Restore Protect Remote.

Current Req value	Description
Lockout Wait To Restore Working	A user initiated a lockout request from the near-end system when the previous request was Wait To Restore Working. The system will ignore line conditions and far-end requests while Lockout Wait To Restore Working is active. The protection line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Wait To Restore Working, and the system will restart the Wait-To-Restore timer with its full time-out value.
Lockout Wait To Restore Working Remote	A user initiated a lockout request from the near-end system when the previous request was Wait To Restore Working Remote. The system will ignore line conditions and far-end requests while Lockout Wait To Restore Working Remote is active. The protection line is the active line. If you execute a Clear Switch Request, the Current Req on the near-end system will return to Wait To Restore Working Remote.
No Request	There are no current protection requests.
Signal Degrade Protect	The system detected a signal degrade condition on the protection line. The signal degrade condition was transmitted by the near-end system and acknowledged by the far-end system. The near-end system continues to send K bytes indicating signal degrade. The working line is the active line.
Signal Degrade Protect Remote	The far-end system has requested a switch to the protection line due to a detected signal degrade on the protection line, and the near-end system has responded. The working line is the active line.
Signal Degrade Protect Request	The near-end system has detected a signal degrade on the protection line. The near-end system has issued a request to the far-end system, but the far-end system has not yet responded. The near-end system will continue with this request indefinitely until the line condition or far-end request changes. The protection line is the active line.

Current Req value	Description
Signal Degrade Working	The system detected a signal degrade condition on the working line. The signal degrade condition was transmitted by the near-end system and acknowledged by the far-end system. The near-end system continues to send K bytes indicating signal degrade. The protection line is the active line.
Signal Degrade Working Remote	The far-end system has requested a switch to the protection line due to a detected signal degrade on the working line, and the near-end system has responded. The protection line is the active line.
Signal Degrade Working Request	The near-end system has detected a signal degrade condition on the working line. The near-end system has issued a request to the far-end system, but the far-end system has not yet responded. The near-end system will continue with this request indefinitely until the line condition or far-end request changes. The working line is the active line.
Trail Signal Fail Protect	The near-end system has detected a trail signal fail on the protection line, and the far-end system has acknowledged it. The near-end system continues to send K bytes indicating trail signal fail. The working line is the active line.
Trail Signal Fail Protect Remote	The far-end system has requested a switch to the protection line due to a detected trail signal fail on the protection line, and the near-end system has responded. The working line is the active line.
Trail Signal Fail Protect Request	The near-end system has detected a trail signal fail condition on the protection line. The near-end system issued a request to the far-end system, but the far-end system has not yet responded. The near-end system will continue with this request indefinitely until the line condition or far-end command changes. The protection line is the active line.
Trail Signal Fail Working	The system detected a trail signal fail on the working line. The trail signal fail was transmitted by the near-end system and acknowledged by the far-end system. The near-end system continues to send K bytes indicating trail signal fail. The protection line is the active line.

Current Req value	Description
Trail Signal Fail Working Remote	The far-end system has requested a switch to the protection line due to a detected trail signal fail on the working line, and the near-end system has responded. The protection line is the active line.
Trail Signal Fail Working Request	The near-end system has detected a trail signal fail condition on the working line. The near-end system has issued a request to the far-end system, but the far-end system has not yet responded. The near-end system will continue with this request indefinitely until the line condition or far-end request changes. The working line is the active line.
Wait To Restore Protect	A line condition has cleared on the protection line, and the Wait-To-Restore timer is running. The working line is the active line.
Wait To Restore Protect Remote	A Wait-To-Restore for the protection line was initiated by the far-end system. The far-end system has signalled the starting of its WTR timer. The working line is the active line.
Wait To Restore Working	A line condition has cleared on the working line, and the WTR timer is running. The protection line is the active line.
Wait To Restore Working Remote	A Wait-To-Restore for the working line was initiated by the far-end system. The far-end system has signalled the starting of its WTR timer. The protection line is the active line.

Related topics For definitions, see “Switch request terms” (10-3).



NTT MSP Current Req priorities

List of priorities

The following list displays the NTT MSP current request values in descending order of priority.

1. Lockout Force Switch Working
2. Lockout Force Switch Working Remote
3. Lockout Force Switch Protect
4. Lockout Force Switch Protect Remote
5. Lockout Trail Signal Fail Working
6. Lockout Trail Signal Fail Working Remote
7. Lockout Trail Signal Fail Protect
8. Lockout Trail Signal Fail Protect Remote
9. Lockout Signal Degrade Working
10. Lockout Signal Degrade Working Remote
11. Lockout Signal Degrade Protect
12. Lockout Signal Degrade Protect Remote
13. Lockout Wait To Restore Working
14. Lockout Wait To Restore Working Remote
15. Lockout Wait To Restore Protect
16. Lockout Wait To Restore Protect Remote
17. Lockout Do Not Revert
18. Lockout No Request
19. Force Switch to Working Request
20. Force Switch to Working
21. Force Switch to Working Remote
22. Force Switch to Protect Request
23. Force Switch to Protect
24. Force Switch to Protect Remote
25. Trail Signal Fail Working Request
26. Trail Signal Fail Working
27. Trail Signal Fail Working Remote
28. Trail Signal Fail Protect Request
29. Trail Signal Fail Protect
30. Trail Signal Fail Protect Remote
31. Signal Degrade Working Request
32. Signal Degrade Working

- 33. Signal Degrade Working Remote
- 34. Signal Degrade Protect Request
- 35. Signal Degrade Protect
- 36. Signal Degrade Protect Remote
- 37. Wait To Restore Working
- 38. Wait To Restore Working Remote
- 39. Wait To Restore Protect
- 40. Wait To Restore Protect Remote
- 41. Do Not Revert
- 42. No Request

Related topic For a definition of priorities, see “Protection switching priorities”
(9-7).



NTT MSP unit condition values

Unit condition value descriptions

The following is a list of possible NTT MSP unit condition values that appear in the Protection Switch - Transmission Query Results window.

Value	Description
Empty Slot	The unit has been removed.
Line Clear	The unit is fully operational.
Signal Degrade	The bit error rate of the multiplex section has exceeded the provisioned threshold for the provisioned number of seconds.
Trail Signal Fail	Failure of the transmission signal (for example: LOS, or AIS) or unit, or the unit has been removed.
Unit Fail	The unit has a failure.

MSP transmission window and procedures

Overview

Purpose Use the MSP transmission window to query the status of, and to request a protection switch for, an MSP group.

Window location *Protection Switch > Transmission > MSP*

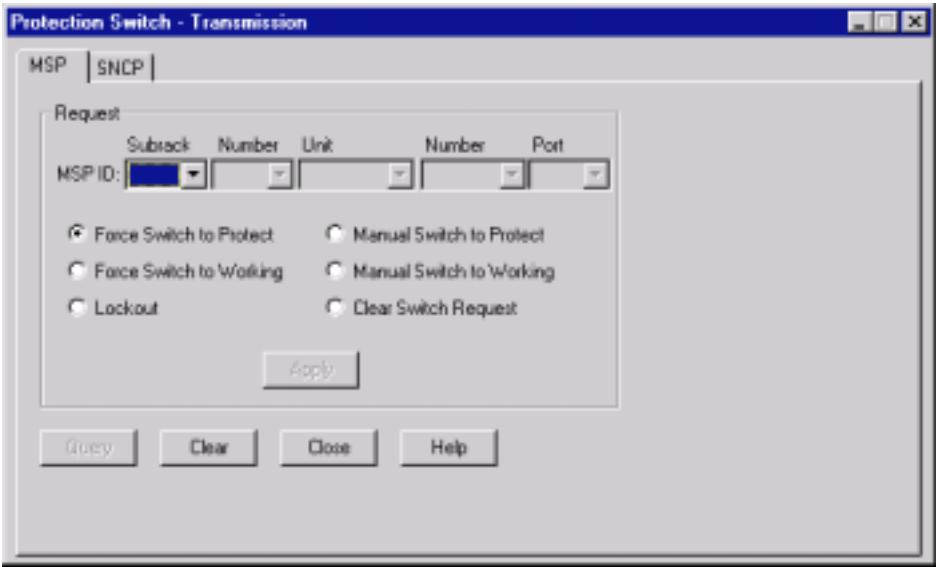
Organisation This section is organised as follows:

- [“MSP transmission window description” \(10-25\)](#)
- [“Querying MSP groups” \(10-28\)](#)
- [“MSP transmission query results” \(10-29\)](#)
- [“Requesting an MSP switch” \(10-31\)](#)



MSP transmission window description

Illustration The following illustration shows the MSP transmission window.



Field descriptions for ITU and ANSI MSP

The MSP transmission window has the following fields.

Field Name	Description
MSP ID	The MSP ID field displays the physical address of the Multiplex Section protection group. For a description of the Multiplex Section protection group IDs, see “MSP addresses” (5-17).
Force Switch to Protect	The Force Switch to Protect field forces service to the protection entity <i>only</i> if the current request is one of the following: • Do Not Revert • Manual Switch to Protect • No Request • Signal Degrade Protect • Signal Degrade Working
Manual Switch to Protect	The Manual Switch to Protect field manually switches service to protection <i>only</i> if the following conditions are true: • The current request is No Request. • The protection entity does <i>not</i> have a failure condition. If the protection entity is already active, it remains active.

Field Name	Description
Force Switch to Working	The Force Switch to Working field forces service to the protection entity <i>only</i> if the current request is one of the following: • Do Not Revert • Manual Switch to Working • No Request • Signal Degrade Protect • Signal Degrade Working This switch will remain in effect until a Clear Switch Request is made or until a higher priority condition occurs.
Manual Switch to Working	The Manual Switch to Working field manually switches service to working <i>only</i> if the following conditions are true: • The current request is Do Not Revert. • The working entity does <i>not</i> have a failure condition. If the working entity is already active, it remains active.
Lockout	The Lockout field locks service off of protection and onto working until someone requests a Clear request.
Clear Switch Request	The Clear Switch Request field clears any of the following previous switch requests: • Force Switch to Protect • Force Switch to Working • Lockout • Manual Switch to Protect • Manual Switch to Working

Field descriptions for NTT MSP

The MSP transmission window has the following fields.

Field Name	Description
MSP ID	The MSP ID field displays the physical address of the Multiplex Section protection group.

Field Name	Description
Force Switch to Protect	The Force Switch to Protect field forces service to the protection entity, regardless of the current state (active, standby, or failed) of the protection entity, but <i>only</i> if the current request is one of the following: • Do Not Revert • No Request • Signal Degrade Protect • Signal Degrade Working If the protection unit is already active, it remains active.
Manual Switch to Protect	The Manual Switch to Protect field is <i>not valid</i> for NTT MSP. The system will return a message if you select this field.
Force Switch to Working	The Force Switch to Working field forces service to the working entity, regardless of the current state (active, standby, or failed) of the working entity, but <i>only</i> if the current request is one of the following: • Do Not Revert • No Request • Signal Degrade Protect • Signal Degrade Working This switch will remain in effect until a Clear Switch Request is made or until a higher priority condition occurs.
Manual Switch to Working	The Manual Switch to Working field is <i>not valid</i> for NTT MSP. The system will return a message if you select this field.
Lockout	The Lockout field locks service in the current state until a Clear condition occurs.
Clear Switch Request	The Clear Switch Request field clears any of the following previous switch requests: • Force Switch to Protect • Force Switch to Working • Lockout

Related topic For general information about windows, see “About the main application window” (4-10).



Querying MSP groups

Procedure

- 1 Go to the MSP transmission window at *Protection Switch > Transmission > MSP*.
-

- 2 Select the MSP address in the MSP ID field.

Reference:

For a description of the MSP addresses, see “MSP addresses” (5-17).

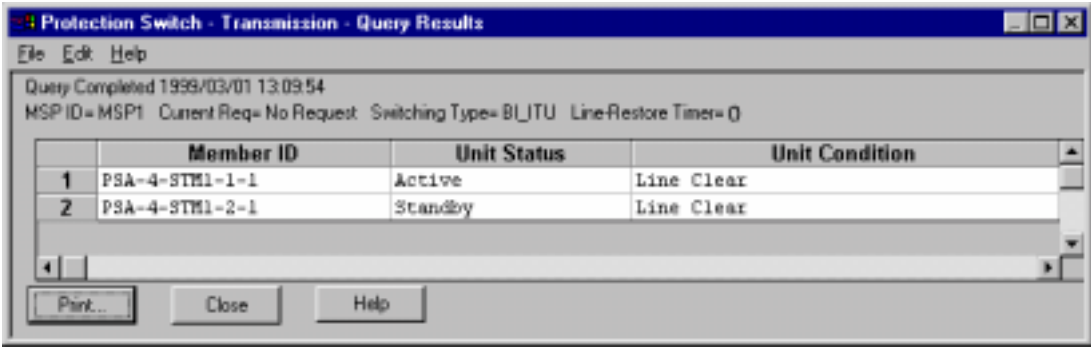
- 3 Click Query.

END OF STEPS



MSP transmission query results

Illustration Use the following illustration only as an example of query results from the MSP transmission window.



Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the MSP transmission Query Results window.

Title	Description
MSP ID	The MSP ID field displays the group ID as MSP{1, 3, 5, 7, 11, 13, 15, 17}.
Current Req	The Current Req displays the current request.
Switching Type	The Switching Type displays the type of MSP as one of the following: • BI_ITU — Bidirectional ITU • UNI_ITU — Unidirectional ITU • BI_NTT — Bidirectional NTT • UNI_ANSI — Unidirectional ANSI
Line Restore Timer	The Line Restore Timer displays the line restore timer setting in minutes. For ITU and ANSI MSP, a zero will always be displayed as the line restore timer value.
Member ID	The Member ID column displays the entity addresses of each member of the group.
Unit Status	The Unit Status column displays the current status as one of the following: • Active • Standby For more information, see “Active and standby” (9-5).

Title	Description
Unit Condition	The Unit Condition column displays the current unit condition for each member of the group as one of the following: • Empty Slot • Line Clear • Signal Degrade • Trail Signal Fail • Unit Fail

Related topics For more information, see one of the following topics:

- “About the main application window” (4-10)
- “Switch request terms” (10-3)
- “ITU and ANSI MSP Current Req values” (10-7)
- “ITU and ANSI MSP Current Req priorities” (10-10)
- “NTT MSP Current Req values” (10-13)
- “NTT MSP Current Req priorities” (10-21)
- “ITU and ANSI MSP unit condition values” (10-11)



Requesting an MSP switch

Procedure

- 1 Go to the MSP transmission window at *Protection Switch > Transmission > MSP*.
-

- 2 Select the desired MSP group address in the MSP ID field.

Reference:

For more information, see “MSP addresses” (5-17).

- 3 Select one of the following switch requests:
 - Force Switch to Protect (all MSP types)
 - Force Switch to Working (all MSP types)
 - Lockout (all MSP types)
 - Manual Switch to Protect (valid for ITU and ANSI MSP only)
 - Manual Switch to Working (valid for ITU and ANSI MSP only)
 - Clear Switch Request (all MSP types)
-

- 4 Click Apply.

END OF STEPS



SNCP current requests, priorities, and unit conditions

Overview

Purpose This section contains the Sub-Network Connection Protection (SNCP) current requests, priorities, and unit condition information.

Organisation This section is organised as follows:

- “SNCP Current Request values” (10-33)
- “SNCP Current Request priorities” (10-34)
- “SNCP unit condition values” (10-35)



SNCP Current Request values

SNCP Current Request value descriptions

The following Current Request information appears at the top of the table in the Protection Switch - Transmission - SNCP Query Results window.

Current Request value	Description
Lockout	A user initiated a switch request that locked the selector on the working trail. This will prevent access to the protection trail until you clear the lockout request.
Freeze	A user initiated a freeze that has locked the trails in their current state.
Force Switch to Working	A user initiated a switch that forced the trail to working.
Force Switch to Protect	A user initiated a switch that forced the trail to protection.
Trail Signal Fail Working	A Trail Signal Fail condition has been detected on the working trail.
Trail Signal Fail Protection	A Trail Signal Fail condition has been detected on the protection trail.
Trail Signal Degrade Working	A Trail Signal Degrade condition has been detected on the working trail.
Trail Signal Degrade Protection	A Trail Signal Degrade condition has been detected on the protection trail.
Manual Switch to Working	A user initiated a switch request that transferred service to the working trail.
Manual Switch to Protect	A user initiated a switch request that transferred service to the protection trail.
Do Not Revert	The selector is on the protection trail after a switch request has cleared. This state applies to only SNCP groups provisioned as nonrevertive switching.
Wait to Restore	A trail signal fail or a trail signal degrade condition has cleared. You will see this state for the provisioned wait-to-restore time.
No Request	There are no current protection requests.

Related topics For definitions, see “Switch request terms” (10-3).



SNCP Current Request priorities

List of priorities The following list displays the SNCP current request values in descending order of priority:

1. Clear
2. Freeze
3. Lockout
4. Forced Switch
5. Trail Signal Fail
6. Signal Degrade
7. Wait to Restore
8. Do Not Revert
9. No Request

Related topic For a definition of priorities, see “Protection switching priorities” (9-7).



SNCP unit condition values

Unit condition descriptions The following is a list of possible SNCP unit condition values that appear in the Protection Switch - Transmission - SNCP Query Results window.

Value	Description
Operational	The unit is operational.
Trail Signal Degrade	The bit error rate of the multiplex section has exceeded the provisioned threshold for the provisioned number of seconds.
Trail Signal Fail	A failure of the transmission signal or unit, or the unit has been removed.



SNCP transmission window and procedures

Overview

Purpose Use the SNCP transmission window to query the status of, and to request a protection switch for, an SNCP group.

Window location *Protection Switch > Transmission > SNCP*

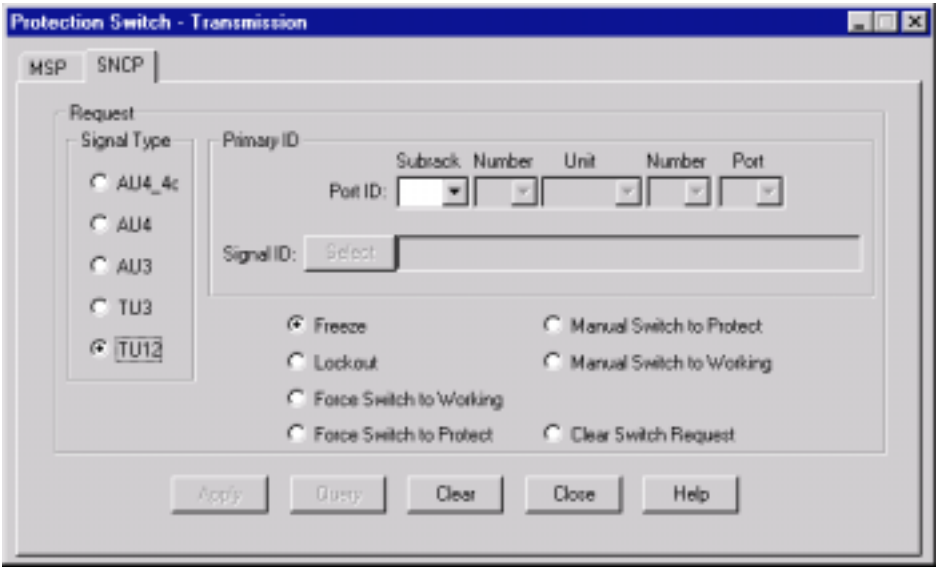
Organisation This section is organised as follows:

- [“SNCP transmission window description” \(10-37\)](#)
- [“Querying SNCP transmission groups” \(10-39\)](#)
- [“SNCP transmission query results” \(10-40\)](#)
- [“Requesting an SNCP switch” \(10-42\)](#)



SNCP transmission window description

Illustration The following illustration shows the SNCP transmission window.



Field descriptions The SNCP transmission window has the following fields.

Field Name	Description
Signal Type	The Signal Type field specifies the signal level as AU4_4c, AU4, AU3, TU3, or TU12.
Primary ID	The Primary ID is the entity that is the preferred routing that traffic travelling from one network element to another normally follows.
Port ID	The Port ID field specifies the physical location of the entity.
Signal ID	The Signal ID field specifies the signal level of the address that you want to switch. The options available for Signal ID depend on the Signal Type. For a description of the Signal ID options, see “About signal layer addresses” (5-4).
Freeze	The Freeze request freezes the current SNCP state as is and will prevent further switches. This request “nests” with other requests. For example, if you request a Freeze when a Force Switch to Protect is in effect, the first Clear you request will clear the Freeze, while the second Clear will clear the Force Switch to Protect.

Field Name	Description
Lockout	Lockout will lock the selector on the working trail and prevent access to the protection trail until someone requests a Clear request.
Force Switch to Working	A Force Switch to Working request transfers service to the working trail unless an equal or higher priority request is in effect. A Force Switch to Working request is effective regardless of the condition of the working trail, since operation is unidirectional and no Automatic Protection Switching (APS) channel communication is required to complete a switch.
Force Switch to Protect	A Force Switch to Protect request transfers service to the protection trail unless an equal or higher priority request is in effect. A Force Switch to Protect request is effective regardless of the condition of the protection trail, since operation is unidirectional and no Automatic Protection Switching (APS) channel communication is required to complete a switch.
Manual Switch to Protect	A Manual Switch to Protect request transfers service to the protection trail unless an equal or higher priority request is in effect.
Manual Switch to Working	A Manual Switch to Working request transfers service to the working trail unless an equal or higher priority request is in effect.
Clear Switch Request	A Clear Switch Request clears any previous user-initiated switch request.

Related topic For general information about windows, see “About the main application window” (4-10).



Querying SNCP transmission groups

Procedure

- 1** Go to the SNCP protection window at *Protection Switch > Transmission > SNCP*.

- 2** Select the Signal Type.

- 3** Select the Primary ID in the Port ID and Signal ID fields.

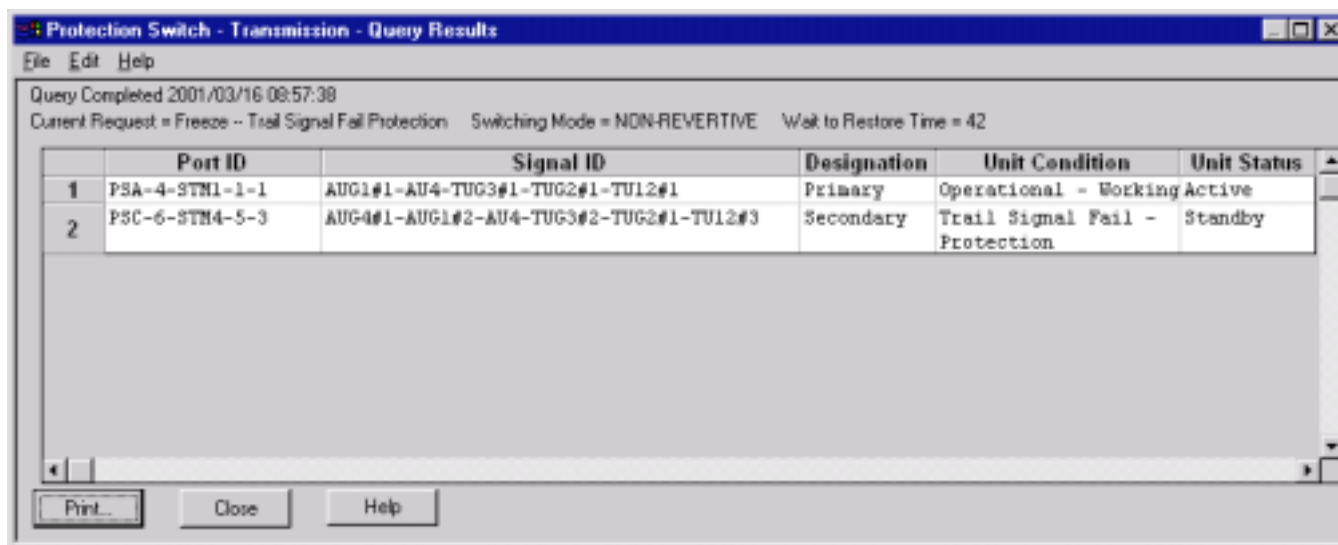
- 4** Click Query.

END OF STEPS



SNCP transmission query results

Illustration Use the following illustration only as an example of query results from the SNCP transmission window.



Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the SNCP transmission Query Results window.

Title	Description
Current Request	This field displays the current request value. For more information, see one of the following: “SNCP Current Request values” (10-33) “SNCP Current Request priorities” (10-34)
Switching Mode	The Switching Mode displays one of the following: - REVERTIVE - NON-REVERTIVE
Wait to Restore Time	The Wait to Restore Time field displays the amount of time (in minutes) that the system waits, after a failure condition that caused a protection switch clears, before switching back to the previously-active trail.
Port ID	The Port ID field displays the physical location of the entity.

Title	Description
Signal ID	The Signal ID field displays the signal level of the entity. For a description of the Signal ID options, see “About signal layer addresses” (5-4).
Designation	The Designation column displays the designation as one of the following: • Primary • Secondary
Unit Condition	The Unit Condition column displays the current unit condition for each member of the group as one of the following: • Operational • Trail Signal Degrade • Trail Signal Fail
Unit Status	The Unit Status column displays the current status as one of the following: • Active • Standby For more information, see “Active and standby” (9-5).

Related topics For more information, see one of the following topics:

- “About the main application window” (4-10)
- “SNCP Current Request values” (10-33)
- “SNCP Current Request priorities” (10-34)
- “SNCP unit condition values” (10-35)



Requesting an SNCP switch

Procedure

- 1 Go to the SNCP transmission window at *Protection Switch > Transmission > SNCP*.

- 2 Select the Signal Type.

- 3 Select the Primary ID in the Port ID and Signal ID fields.

- 4 Select one of the following switch requests:
 - Freeze
 - Lockout
 - Force Switch to Working
 - Force Switch to Protect
 - Manual Switch to Protect
 - Manual Switch to Working
 - Clear Switch Request

- 5 Click Apply.

END OF STEPS





11 Controller maintenance

Overview

- Purpose** “Controller maintenance” contains the following information:
- General information about performing maintenance on the controllers (MPUs and SRCs)
 - Descriptions of the windows that are used for controller maintenance
 - Step-by-step procedures for the following:
 - Querying a controller
 - Removing a controller from service
 - Restoring the database software on an MPU
 - Restoring the MPU to service without reloading database software
 - Initialising a unit

- Organisation** “Controller maintenance” is organised as follows:
- “Background information” (11-2)
 - “Subrack Control window and procedures” (11-14)
 - “Unit Control window and procedures” (11-37)



Background information

Overview

Purpose This section contains general information about controllers.

Organisation This section is organised as follows:

- “Controller maintenance tasks” (11-3)
- “Controller maintenance terms” (11-4)
- “Differences between cold and warm starts” (11-5)
- “About the MPU out-of-service state” (11-6)
- “About the SRC out-of-service state” (11-7)
- “Master and slave units” (11-8)
- “SRC states” (11-9)
- “Unit states” (11-11)
- “Unit ID values” (11-13)



Controller maintenance tasks

Subrack control tasks The following tasks are performed from the Subrack Control window:

- “Querying an MPU controller” (11-16)
- “Removing the MPU on a duplicated MC configuration” (11-18)
- “Querying an SRC” (11-16)
- “Restoring an SRC to service” (11-35)
- “Recovering from a Wrong unit in slot state” (11-36)

Unit control tasks The following tasks are performed from the Unit Control window:

- “Performing a warm start” (11-41)
- “Performing a cold start” (11-42)



Controller maintenance terms

- List of terms**
- Boot** A boot transfers the contents of backup memory into working memory. Booting usually occurs when a unit or controller is inserted, when the system is powered up, or when a subrack is created.
- Cold start** A cold start initialises or recovers a single unit. A cold start may affect service.
- Controller** Controller is another name for the SRC and MPU units. Controllers administer the other units on their respective subracks.
- Initialisation** An initialisation is a restart that synchronises the hardware with the software. Warm and cold starts are also called initialisations.
- Master unit** A master unit is a unit that controls a slave unit by sending messages or writing registers to the slave. BSC, DTU, and port units are master units.
- Slave unit** A slave unit is a unit that is controlled by a master unit. BSSUs, BSIUs, and IUs are slave units.
- Warm start** A warm start initialises or recovers a single unit or a group of units without affecting service.



Differences between cold and warm starts

Definition A warm or cold start, also called an initialisation, synchronises the hardware with the software.

Differences between cold and warm starts The following table describes the differences between warm and cold starts when using the Unit Control window to initialise a unit.

Warm starts	Cold starts
Initialise or recover a single unit or group of units	Initialise or recover only a single unit and its slave (if applicable)
Are available on a specific unit address or an address with ALL in a subfield	Are available only on a specific unit address
Are nonservice-affecting unless the cross connect data in the database does not match the hardware	Are potentially service-affecting on active units ¹ for the following reasons: • Runs tests and initialises all of the unit hardware • Causes a glitch on all cross connects on the unit

Notes:

1. A cold start on standby units does not affect service.



About the MPU out-of-service state

MPU OOS on a single MC configuration

When you put an MPU controller on a single Main Controller (MC) in the out-of-service (OOS) state, the following will happen:

- The MPU cannot run application software. This means that the user interface will no longer function.
- The system will also put the SRCs in the Matrix/Synchronisation and port subracks in the out-of-service state.
- The MPU will restore itself up to the firmware, and you must continue the restoral from the firmware prompt.

MPU OOS on a duplicated MC configuration

When you put an MPU controller on a duplicated Main Controller (MC) in the out-of-service state (OOS), the user interface will still function. The MPU does not automatically attempt to restore itself to service. You must restore the MPU from the Subrack Control window.

Why remove the MPU from service?

Remove the MPU from service to do any of the following:

- Safely remove units on the Main Controller subrack
- Execute a system-wide warm start after booting the MPU
- Load a new software release
- Perform database restorals. You can perform database backups without placing the MPU in the out-of-service state.

Tip Putting an MPU controller in the out-of-service state is also called removing the MPU from service.



About the SRC out-of-service state

Description of SRC out-of-service state

When you put an SRC controller in the out-of-service state (OOS), the user interface will still function. The SRC does not automatically attempt to restore itself to service. You must restore the SRC from the Subrack Control window.

Tip

Putting an SRC controller in the out-of-service state is also called removing the SRC from service.

Why remove the SRC from service?

Remove the SRC from service to do any of the following:

- Safely replace SRC units
- Change the provisioning on a port subrack from one type of port subrack to another (for example: change from a PSA subrack to a PSC subrack)
- Delete a subrack



Master and slave units

Initialising master and slave units

Whenever you initialise a master unit, the system also initialises the associated slave units. You can initialise slave units independently of the master unit, with the exception of the Interface Unit (IU).

Table of master and slave units

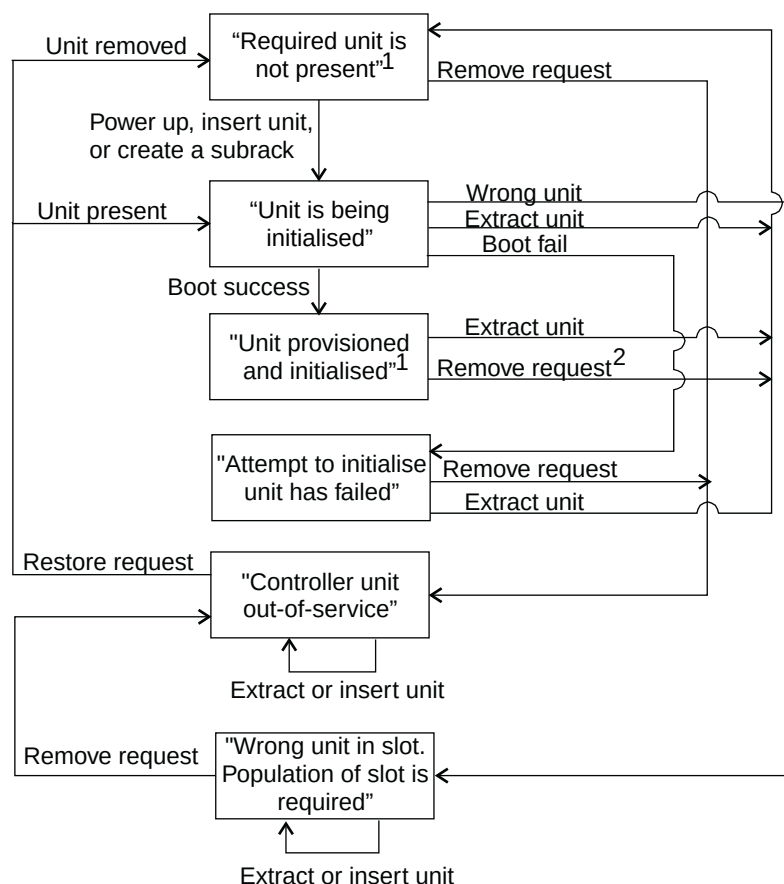
The following is a table of the master and slave units.

Master	Slave
Active BSC	All 10 BSSUs
BSC-1	OLU 1 and 2
BSC-2	OLU 3 and 4
Active DTU	All 10 BSIUs
STM-1	IU



SRC states

Graphic of SRC states The following is a graphic of all the possible SRC states.



Legend:

1. Transitions into and out of this state will cause the system to generate an autonomous report.
2. If the system has both active and standby MS subracks, and you want to remove the currently-active SRC, the system will not accept the remove request until you first switch service to the standby SRC. This will make the SRC you want to remove the standby SRC.

Description of SRC states The following table describes all of the possible SRC states.

Screen display	State	Description
Attempt to initialise unit has failed	BOOT_FAIL	The SRC initialisation failed.

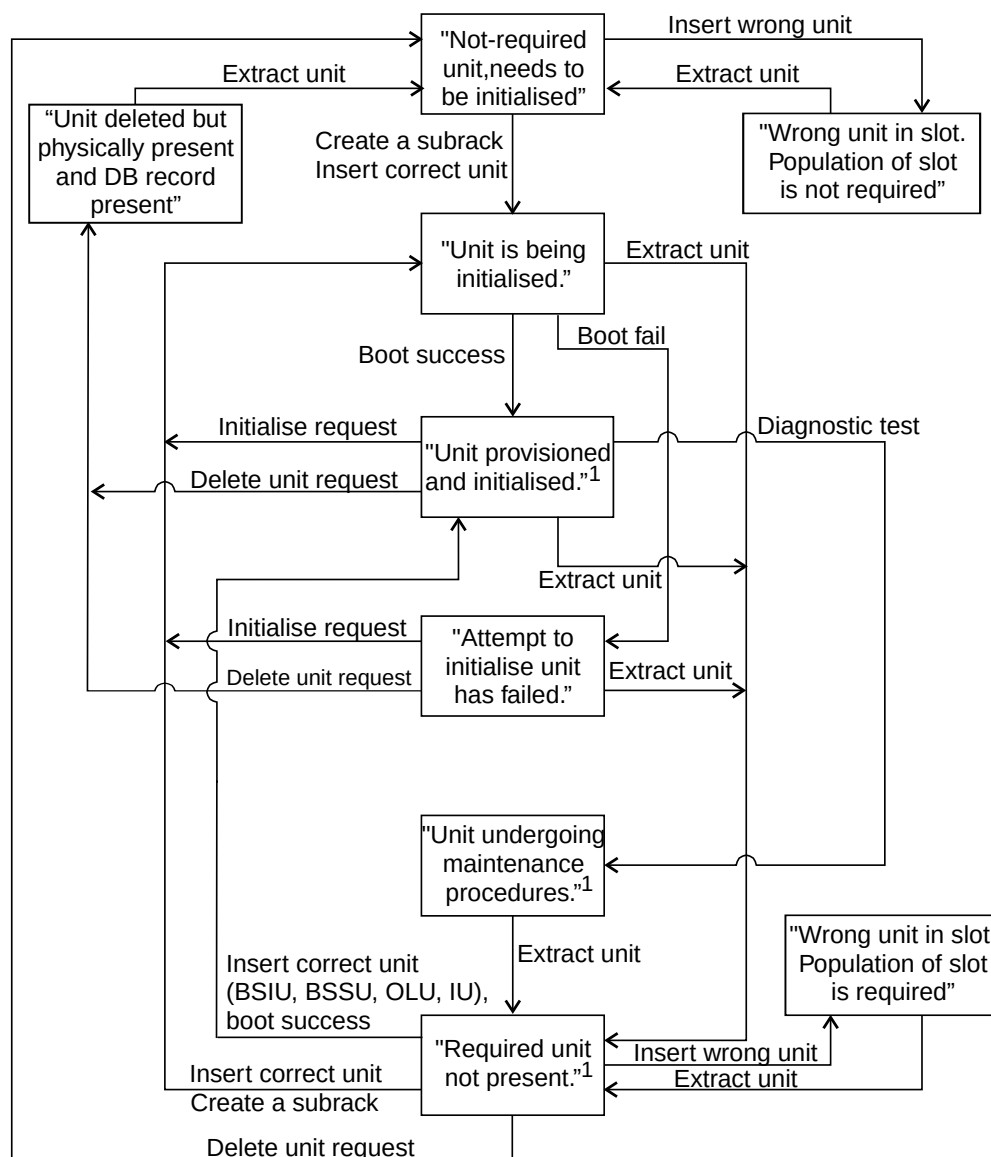
Screen display	State	Description
Unit is being initialised	BOOTING	The entire subrack is in the process of booting and has not yet finished.
Controller unit out of service	DBOOS	The SRC has been manually placed out of service using the Remove button on the Subrack Control window. The only way to initialise the SRC again (usually referred to as re-initialising) is to restore it using the Subrack Control window. Reseating the SRC unit will not cause the unit to re-initialise, nor will reseating the unit remove it from the DBOOS state.
Unit provisioned and initialised	EQPD	The entire subrack has been successfully initialised or recovered. The SRC unit is fully operational in this state.
Required unit is not present	UNEQPD	The MCLAN link is lost. Specifically, this could mean that any of the following events occurred: • The SRC was physically removed from the subrack. • The MCLAN link was disconnected. After you insert an SRC unit, the SRC may remain in the UNEQPD state for a few minutes until the SRC completes initialisation.
Wrong unit in slot. Population of slot is required	WRONG_UNIT_UN	An SRC unit with the wrong apparatus code was inserted into a slot. The unit is required. To recover the SRC unit from this state, see “Recovering from a Wrong unit in slot state” (11-36).



Unit states

Graphic of unit states

The following is a graphic of all the possible unit states for the STU and the master and slave units. You can view these states by querying the Unit window at *Provision > Equipment > Unit*.



Notes:

- Transitions into or out of this state will result in an autonomous message. Query the autonomous messages window at *Reports > Autonomous Messages* and select Unit State Changes in the Message/Event Type field.

Description of STU, master, and slave unit states

Units have the following possible states.

Screen display	State	Description
Attempt to initialise unit has failed	BOOT_FAIL	The unit initialisation failed.
Unit is being initialised	BOOTING	The entire subrack is in the process of booting and has not yet finished.
Not-required unit, needs to be initialised	DBAVAIL	The unit has never been booted in the subrack. Due to the way the system autoprovisions after a subrack creation, a database record will exist for the unit, even if the unit is not yet physically present.
Unit provisioned and initialised	EQPD	The entire subrack has been successfully initialised or recovered. The unit is fully operational in this state.
Required unit is not present	UNEQPD	The MCLAN link is lost. Specifically, this means that the required unit was physically removed from the subrack or it was never inserted.
Wrong unit in slot. Population of slot is not required	WRONG_UNIT_AV	A unit with the wrong apparatus code was inserted into a slot. The unit is not required. The system will not generate any alarms when the unit is extracted from the subrack.
Wrong unit in slot. Population of slot is required	WRONG_UNIT_UN	A unit with the wrong apparatus code was inserted into a slot. The unit is required. The system will generate alarms when the unit is extracted from the subrack.



Unit ID values

Table of Unit ID values

The Unit ID field specifies the physical address of the unit. The following table describes all of the possible Unit ID addresses and whether you can warm start or cold start the equipment at that address.

Unit ID address	Warm start?	Cold start?
MS-3-STU-{ACTIVE, STANDBY, 1, 2}	Yes	Yes
MS-3-BSC-{ACTIVE, STANDBY, 1, 2}	Yes	Yes
MS-3-BSSU-{1-10}	No	Yes
{PSA, PSC}-{4-11, 4-19}-DTU-{1, 2}	Yes	Yes
{PSA, PSC}-{4-11, 4-19}-DTU-ALL	Yes	No
{PSA, PSC}-{4-11, 4-19}-BSIU-{1-10}	No	Yes
{PSA, PSC}-{4-11, 4-19}-ALL-ALL	Yes	No
PSA-{4-11, 4-19}-STM1-{1-9, 11-19}	Yes	Yes
PSA-{4-11, 4-19}-STM1-ALL	Yes	No
PSC-{4-11, 4-19}-STM4-{1-8}	Yes	Yes
PSC-{4-11, 4-19}-STM4-ALL	Yes	No
PSC-{4-11, 4-19}-STM16-{1-8}	Yes	Yes
PSC-{4-11, 4-19}-STM16-ALL	Yes	No



Subrack Control window and procedures

Overview

Purpose Use the Subrack Control window to query a controller state or to remove or restore an MPU or an SRC.

Window location *Maintenance > Controller Maintenance > Subrack Control*

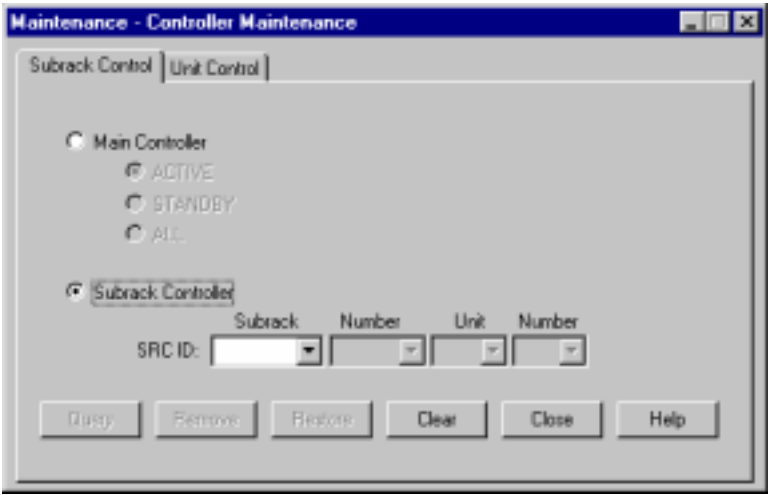
Organisation This section is organised as follows:

- [“Subrack Control window description” \(11-15\)](#)
- [“Querying an MPU controller” \(11-16\)](#)
- [“Querying an SRC” \(11-16\)](#)
- [“Subrack Control query results” \(11-17\)](#)
- [“Removing the MPU on a duplicated MC configuration” \(11-18\)](#)
- [“Removing the MPU on a single MC configuration” \(11-22\)](#)
- [“Restoring the DB on an MPU with a duplicated MC configuration” \(11-23\)](#)
- [“Restoring the DB on an MPU with a single MC configuration” \(11-29\)](#)
- [“Removing an MS subrack SRC from service” \(11-33\)](#)
- [“Removing a port subrack SRC from service” \(11-34\)](#)
- [“Restoring an SRC to service” \(11-35\)](#)
- [“Recovering from a Wrong unit in slot state” \(11-36\)](#)



Subrack Control window description

Illustration The following illustration shows the Subrack Control window.



Field descriptions The Subrack Control window has the following fields.

Field name	Description
Main Controller	The Main Controller field is used to specify the Main Controller as one of the following: • ACTIVE • STANDBY • ALL
Subrack Controller and SRC ID	The SRC ID in conjunction with the Subrack Controller radio button is used to specify the Subrack Controller (SRC) entity address. For more information about SRC addresses, see one of the following topics: • “MS entity addresses” (5-12) • “PSA entity addresses” (5-13) • “PSC entity addresses” (5-14) • “Wildcard addresses” (5-9)

Related topic For general information about windows, see “About the main application window” (4-10).



Querying controllers

Querying an MPU controller

- 1 Go to the Subrack Control window at *Maintenance > Controller Maintenance > Subrack Control*.
- 2 Click on Main Controller.
- 3 Select Active, Standby, or ALL.
- 4 Click Query.

END OF STEPS

Querying an SRC

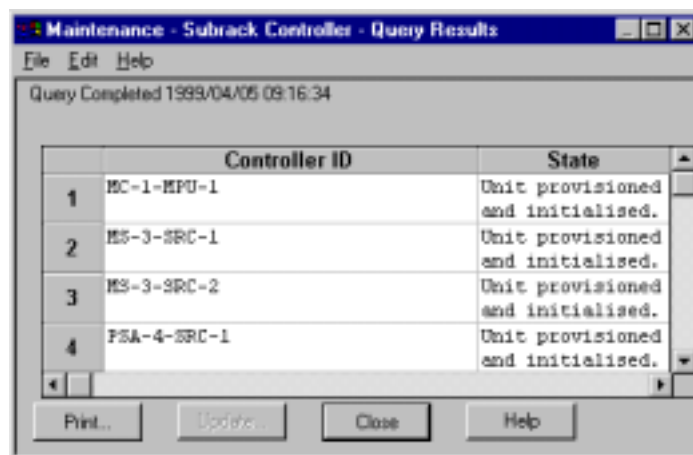
- 1 Go to the Subrack Control window at *Maintenance > Controller Maintenance > Subrack Control*.
- 2 Click on Subrack Controller.
- 3 Select the address of the SRC in the SRC ID field.
- 4 Click Query.

END OF STEPS



Subrack Control query results

Illustration Use the following illustration only as an example of query results from the Subrack Controller window.



Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the Subrack Controller Query Results window.

Column	Description
Controller ID	The Controller ID column displays the Controller ID of the entity you queried.
State	The State field column the current controller state. For a description of the SRC states, see “SRC states” (11-9).

Related topic For general information about windows, see “About the main application window” (4-10).



Removing the MPU on a duplicated MC configuration

Purpose Use this procedure to remove the MPU on a system configured with a duplicated Main Controller (MC). You must use this procedure to remove the MPU so that you can perform various maintenance procedures.

Examples

The following are examples of maintenance procedures that require you to remove the MPU:

- Replace a defective MPU
- Perform an upgrade
- Load software

Before you begin To perform this procedure, you must have the following:

- A Magneto Optical (MO) disk containing a recent database backup.
- A console terminal connected to WS-1 or WS-2 on the User Panel.

Related topics

For more information, see any of the following topics:

- “Backing up the system database” (18-3)
- “About the MPU out-of-service state” (11-6)

Procedure

- 1 Query the Main Controller (MC) protection status to make sure that the MPU you want to replace is located on the standby MC.

Reference:

Go to *Protection > Equipment > MC Control*.

- 2 Choose one of the following:

If the MPU is located on the	Then
Standby MC	Go to the next step.
Active MC	Switch service to standby before going to the next step. Reference: For more information, see “Requesting an MC protection switch” (9-71).

-
- 3** Make sure that your console terminal is connected to the *active* MC.
-

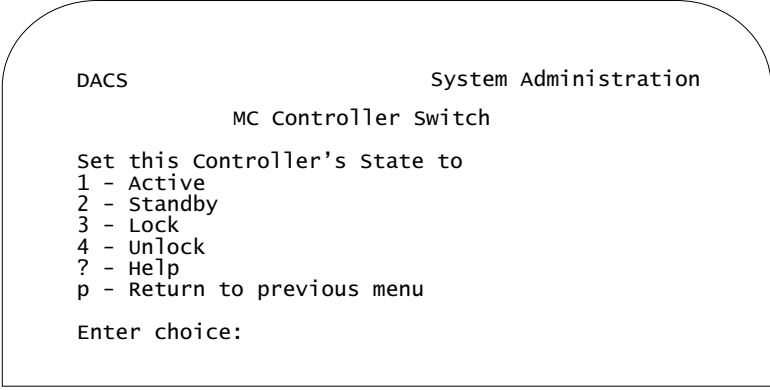
- 4** From the console terminal, go to the MC Duplication Functions screen.

Reference:

For more information, see “Getting to the MC Duplication Functions screen” (9-68).

- 5** Press **2** (Switch MC Controller).

Result:



```
DACS                               System Administration
                                MC Controller Switch

Set this Controller's State to
1 - Active
2 - Standby
3 - Lock
4 - Unlock
? - Help
p - Return to previous menu

Enter choice:
```

-
- 6** From the MC Controller Switch screen, press **3** (Lock).
-

- 7** Press **p** (Return to previous menu).

Result:

The MC Duplication Functions screen reopens.

- 8** Press **1** (Query Duplication Status), and make sure the MC status is “Locked”.
-

- 9** From the DACS user interface, go to *Maintenance > Controller Maintenance > Subrack Control*, and remove the standby MC from service.

1. Select Main Controller.
2. Select STANDBY.
3. Click Remove.

10 Press the green power button on the standby MC.

11 Perform the appropriate maintenance event, such as replacing a
defecting MPU or upgrading the database.

12 Press the green power button again on the standby MC.
This will power up the standby MC.

13 Connect the console terminal to the *standby* MC.

14 At the PPC1-Diag> prompt on the terminal, type `pboot 0 0` and
then press **ENTER**
This will start the process to boot the standby MC.

15 Let the standby MC boot without stopping the boot process.
If the booting process stops at the Pre-NEF Services menu, press **c**
(Continue Booting).

Result:

The standby MC is completely booted when the screen displays
one of the following messages:

- `w001 Software Initialisation Complete` — if
MC-1 is standby
 - `w002 Software Initialisation Complete` — if
MC-2 is standby
-

16 Connect the console terminal to the *active* MC.

17 From the console terminal, go to the MC Duplication Functions
screen.

Reference:

For more information, see “Getting to the MC Duplication
Functions screen” (9-68).

18 Press **2** (Switch MC Controller).

Result:

The MC Controller Switch screen reopens.

-
- 19** From the MC Controller Switch screen, press **4** (Unlock).
-

- 20** Press **p** (Return to previous menu).

Result:

The MC Duplication Functions screen reopens.

-
- 21** Press **1** (Query Duplication Status), and make sure that the MC status is “Unlocked”.

END OF STEPS



Removing the MPU on a single MC configuration

Purpose Use this procedure to remove the MPU from the software on a system configured with a single Main Controller (MC).

Before you begin Make sure you have a recent database backup on a Magneto Optical (MO) disk before removing the MPU.

Related topics

For more information, see any of the following topics:

- “Backing up the system database” (18-3)
- “About the MPU out-of-service state” (11-6)

Procedure **Important!** This procedure will save any recent changes to the hard disk. If you press the reset button on the MC subrack instead of performing this procedure, these changes may not be saved.

1 Go to the Subrack Control window at *Maintenance > Controller Maintenance > Subrack Control*.

2 Click on Main Controller.

3 Click Remove.

Result:

The system displays a confirmation message.

4 Click yes to continue.

Result:

For a single MC configuration, the MPU is removed from service and the user-interface session is disconnected.

END OF STEPS



Restoring the DB on an MPU with a duplicated MC configuration

Purpose The following procedure explains how to restore the database from a previously-made backup Magneto Optical (MO) disk. Use this procedure for a duplicated Main Controller (MC) configuration.

Before you begin To perform this procedure, you must have the following:

- An MO disk containing a recent database backup that you want to use to overwrite the current database.
- A terminal connected to WS-1 on the User Panel.

Procedure

1 Query the MC protection status.

Reference:

Go to *Protection > Equipment > MC Control*.

2 Choose one of the following:

If MC-1 is	Then
Active	Go to the next step.
Standby	Switch service to active before going to the next step. Reference: For more information, see “Requesting an MC protection switch” (9-71).

3 Remove the standby MC from service.

Reference:

Go to *Maintenance > Controller Maintenance > Subrack Control*.

Important! You will lose the user interface after doing this step.

4 Remove the active MC from service.

Reference:

Go to *Maintenance > Controller Maintenance > Subrack Control*.

-
- 5** Go to the console terminal.

Make sure it is connected to the *active* MC.

- 6** At the PPC1-Diag> prompt on the terminal, type `pboot 0 0` and then press **ENTER**

Result:

```
Booting from NCR53C825, Controller 0, Drive 0
```

```
.  
.  
.
```

```
Press any key to enter the software  
administration menu.  
You have 10 seconds to do this...
```

-
- 7** Press the space bar to see the software administration (Pre-NEF Services) menu.

Result:

```
DACS
```

```
System Administration
```

```
Pre-NEF Services
```

```
1. - Database/System Backup  
2. - Database/System Restore  
3. - Database Upgrade from 2.1  
? - Help  
c - Continue Booting  
q - Quit Without Booting
```

```
Enter choice:
```

-
- 8** Press **2** (Database/System Restore), and then press **ENTER**

Result:

```
Restore copies files from the MO to the MC hard
disk.
Files stored on the MC hard disk will be
replaced with the MO version.
ARE YOU sure <y,n>>
```

-
- 9** Press **y** to confirm, and then press **ENTER**

Result:

The following screen displays after several minutes.

```
Please insert the MO disk for Restore.
Hit <Return> when complete >
```

-
- 10** Insert the backup MO disk into the MO drive of the *active* MPU.

Reference:

For a procedure describing how to insert an MO disk, see
“About MO disks” (2-7).

-
- 11** Press **ENTER**

Result:

```
checking for presence of MO Please be patient...
MO is present.
Checking to see if the MO has a valid DB backup...
Valid DB on MO
Checking SYS_CON on MO...
Database information on MO disk:
    Frame ID is 0
    Software ID is 4160
    Last backup time is Jul 9 22:15
Database information on frame:
    Frame ID is 7
    Software ID is 6144
    Current time is Jul 9 22:17:15
Do you want to continue the restore <y,n> >
```

-
- 12** Press **y** to confirm, and then press **ENTER**

Result:

```
{Long screen display deleted}

DACS                               System Administration
                                Pre-NEF Services
1. - Database/System Backup
2. - Database/System Restore
3. - Database Upgrade from 2.1
? - Help
c - Continue Booting
q - Quit Without Booting

Enter choice:
```

-
- 13** Remove the backup MO disk from the MO drive of the MPU.

Important! After you complete the following step, the user name prompt may appear before the output response is fully completed. Do *not* enter a login at the user name prompt at this time.

- 14** Press **c** (Continue Booting), and then press **ENTER**

Result:

It will take approximately 10–20 minutes for the following output to complete.

```
{Long screen display deleted}
User name: Booting NEF Software Release B2.1.x 2001/
03/24 08:42:26
w001 Run Level: SYSTEM
w001 Run Level: SYSTEM_ACTIVE
w001 Run Level: BOOT

w001 Run Level: ACTIVE_NEF
w001 Run Level: ACTIVE_ALL
Thu Apr 19 09:18:19 2001 GEN002 dacs6: w001 software
Initialisation Complete.
```


.....
15 Press **ENTER** when the screen displays one of the following messages:

- w001 Software Initialisation Complete — if the restoring database is on MC-1
- w002 Software Initialisation Complete — if the restoring database is on MC-2

Result:



.....
16 Verify that you can log into the active MC using the user interface.

.....
17 Connect the console terminal to the *standby* MC.

.....
18 At the PPC1-Diag> prompt on the terminal, type `pboot 0 0` and then press **ENTER**

This will start the process to boot the standby MC.

.....
19 Let the standby MC boot without stopping the boot process.

If the booting process stops at the Pre-NEF Services menu, press **c** (Continue Booting).

Result:

The standby MC is completely booted when the screen displays one of the following:

- w001 Software Initialisation Complete — if the restoring database is on MC-1
- w002 Software Initialisation Complete — if the restoring database is on MC-2

.....
END OF STEPS
.....

Important!

You do *not* have to restore the database on the standby MC.



Restoring the DB on an MPU with a single MC configuration

Purpose The following procedure explains how to restore the database from a previously-made backup Magneto Optical (MO) disk. Use this procedure for a single MC configuration

Before you begin To perform this procedure, you must have the following:

- An MO disk containing a recent database backup that you want to use to overwrite the current database.
- A terminal connected to WS-1 on the User Panel.

You must also have performed the procedure for removing an MPU.

Related topic

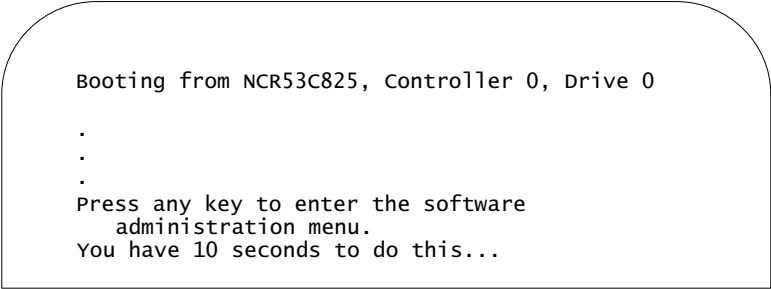
For more information, see “Removing the MPU on a single MC configuration” (11-22).

On a single MC configuration

Important! You will not see the firmware prompt unless you removed the MPU.

- 1 At the PPC1-Diag> firmware prompt on the terminal, type `pboot 0 0` and then press **ENTER**

Result:



```
Booting from NCR53C825, Controller 0, Drive 0
.
.
.
Press any key to enter the software
administration menu.
You have 10 seconds to do this...
```

The command, `pboot 0 0` tells the system to boot the MSU.

- 2 Press the space bar to see the software administration menu.

Result:

```
DACS                                System Administration
                                Pre-NEF Services

1. - Database/System Backup
2. - Database/System Restore
3. - Database Upgrade from 2.1
? - Help
c - Continue Booting
q - Quit Without Booting

Enter choice:
```

-
- 3** Press **2** (Database/System Restore) and then press **ENTER**

Result:

```
Restore copies files from the MO to the MC hard
disk.
Files stored on the MC hard disk will be
replaced with the MO version.
ARE YOU sure <y,n>
```

-
- 4** Press **y** to confirm, and then press **ENTER**

Result:

The following screen appears after several minutes.

```
Please insert the MO disk for Restore.
Hit <Return> when complete >
```

-
- 5** Insert the backup Magneto Optical disk into the Magneto Optical drive of the MPU.

Reference:

For a procedure describing how to insert a Magneto Optical disk, see “About MO disks” (2-7).

-
- 6** Press **ENTER**

Result:

```
Checking for presence of MO Please be patient...
MO is present.
Checking to see if the MO has a valid DB backup...
Valid DB on MO
Checking SYS_CON on MO...
Database information on MO disk:
    Frame ID is 0
    Software ID is 4160
    Last backup time is Jul 9 22:15
Database information on frame:
    Frame ID is 7
    Software ID is 6144
    Current time is Jul 9 22:17:15
Do you want to continue the restore <y,n> >
```

-
- 7 Press **y** to confirm, and then press **ENTER**

Result:

```
{Long screen display deleted}

DACS                               System Administration
                                   Pre-NEF Services

1. - Database/System Backup
2. - Database/System Restore
3. - Database Upgrade from 2.1
? - Help
c - Continue Booting
q - Quit Without Booting

Enter choice:
```

-
- 8 Remove the backup Magneto Optical disk from the Magneto Optical drive of the MPU.
-

Important! After you complete the following step, the user name prompt may appear before the output response is fully completed. Do *not* enter a login at the user name prompt at this time.

- 9 Press **c** (Continue Booting), and then press **ENTER**

It will take approximately 10–20 minutes for the following output to complete.

Result:

```
{Long screen display deleted}
User name:Booting NEF Software Release B2.1.x 2001/
03/24 08:42:26
w001 Run Level: SYSTEM
w001 Run Level: SYSTEM_ACTIVE
w001 Run Level: BOOT

w001 Run Level: ACTIVE_NEF
w001 Run Level: ACTIVE_ALL
Thu Apr 19 09:18:19 2001 GEN002 dacs6: w001 Software
Initialisation Complete.
```

-
- 10** When the screen displays Software Initialisation Complete, press **ENTER**

Result:

User name:

-
- 11** Return to the user interface.

END OF STEPS



Removing an MS subrack SRC from service

Before you begin You cannot remove the active SRC in the Matrix and Synchronisation (MS) subrack from service as long as the standby SRC is equipped. Remove the standby SRC from service before you attempt to remove the active SRC from service.

Procedure

- 1 Query the current status of MS Control at *Protection > Equipment > MS Control*.

- 2 Is the SRC that you want to remove from service active or standby?

If	Then
Active	Go to Step 3.
Standby	Go to Step 4.

- 3 Is the active SRC working or protection?

If	Then
Working	Perform a Force Switch to Protect.
Protection	Perform a Force Switch to Working.

- 4 Go to the Subrack Control window at *Maintenance > Controller Maintenance > Subrack Control*.

- 5 Click on the Subrack Controller button.

- 6 Select the address of the SRC in the SRC ID field.

- 7 Click Remove.

Result:

The system displays a confirmation message.

- 8 Click yes to continue.

END OF STEPS



Removing a port subrack SRC from service

Procedure

- 1** Go to the Subrack Control window at *Maintenance > Controller Maintenance > Subrack Control*.

- 2** Click on the Subrack Controller button.

- 3** Select the address of the SRC in the SRC ID field.

- 4** Click Remove.

Result:

The system displays a confirmation message.

- 5** Click yes to continue.

END OF STEPS



Restoring an SRC to service

Procedure

- 1** Go to the Subrack Control window at *Maintenance > Controller Maintenance > Subrack Control*.

- 2** Click on the Subrack Controller button.

- 3** Select the address of the SRC in the SRC ID field.

- 4** Click Restore.

END OF STEPS



Recovering from a Wrong unit in slot state

Purpose Use the following procedure to clear a “Wrong unit in slot” state on an SRC unit. Reseating the SRC unit does *not* cause the unit to re-initialise nor will reseating the unit clear the “Wrong unit in slot” state.

Procedure

- 1 Remove the SRC from service.

Reference: For more information, see one of the following topics:

- “Removing an MS subrack SRC from service” (11-33)
 - “Removing a port subrack SRC from service” (11-34)
-

- 2 Remove the incorrect SRC from the subrack.
-

- 3 Insert the correct SRC.
-

- 4 Restore the SRC to service using the Subrack Control window.

END OF STEPS

.....



Unit Control window and procedures

Overview

Purpose Use the Unit Control window to initialise (in other words to warm start or cold start) a unit's controller or a group of units.

Window location *Maintenance > Controller Maintenance > Unit Control*

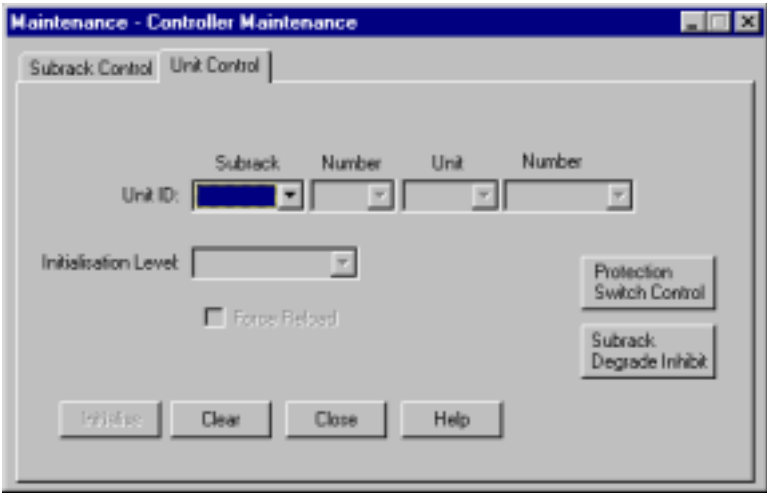
Organisation This section is organised as follows:

- "Unit Control window description" (11-38)
- "Initialising an SRC" (11-40)
- "Performing a warm start" (11-41)
- "Performing a cold start" (11-42)
- "Performing a cold start when the corresponding mate has a failure" (11-44)



Unit Control window description

Illustration The following illustration shows the Unit Control window.



Field descriptions The Unit Control window has the following fields.

Field name	Description
Unit ID	The Unit ID field specifies the physical address of the unit. For more information about the allowable values in this field, see “Unit ID values” (11-13).
Initialisation Level	The Initialisation Level field specifies whether you want to request a warm start or cold start for a particular unit or group of units. For more information, see “Definition” (11-5).
Force Reload	The Force Reload field will become active if the Initialisation Level is COLD and if the unit is a BSC, DTU, STU, or port unit. • If you choose to check the Force Reload box, the system will force a download of a new firmware image into the specified unit even if the new firmware image is the same as the current firmware image. Use this option when the cold start, without force reload, failed. • If you choose <i>not</i> to check the Force Reload box, the system will determine if the unit has the most recent firmware image in place and will load new firmware only if necessary.

Related topic For general information about windows, see “About the main application window” (4-10).



Initialising an SRC

Purpose The following procedure will initialise an SRC by performing a warm start on all the units in the subrack.

Procedure

- 1 Remove the SRC from service.

Reference: For more information, see one of the following topics:

- “Removing an MS subrack SRC from service” (11-33)
 - “Removing a port subrack SRC from service” (11-34)
-

- 2 Restore the SRC to service.

Reference:

For more information, see “Restoring an SRC to service” (11-35).

END OF STEPS

.....



Performing a warm start

Purpose Use the following procedure to perform a warm start. You can warm start STU, BSC, DTU, and port units.

Related topic
For more information, see “Differences between cold and warm starts” (11-5).

Before you begin For an initialisation to work, the hardware must have been initialised at least once during power-up initialisation. The system will only warm start units that are equipped, or that are in the boot fail state. Query the unit state at *Provision > Equipment > Unit*, and verify that the unit is in one of the following states:

- Unit provisioned and initialised (equipped)
- Attempt to initialise unit has failed (boot fail)
- Unit deleted but physically present and DB record present

Related topic
For more information, see “Unit states” (11-11).

- Procedure**
- 1 Go to the Unit Control window at *Maintenance > Controller Maintenance > Unit Control*.
 - 2 In the Unit ID field, select the address of the unit you want to warm start.
 - 3 Select WARM in the Initialisation Level field.
 - 4 Click Initialise.
- END OF STEPS



Performing a cold start

Purpose You can cold start STU, BSC, BSSU, DTU, BSIU, and port units. You **cannot** cold start an address with ALL. Use a cold start when clearing INVcDPLL and INVcFPGA alarms.

Related topic

For more information, see “Differences between cold and warm starts” (11-5).

Before you begin For an initialisation to work, the hardware must have been initialised at least once during power-up initialisation. The system will only cold start units that are equipped, that are in the boot fail state, or that are deleted.

- 1 Query the unit state at *Provision > Equipment > Unit*, and verify that the unit is in one of the following states:
 - Unit provisioned and initialised (equipped)
 - Attempt to initialise unit has failed (boot fail)
 - Unit deleted but physically present and DB record present (A cold start will restart a deleted unit without having to reseat the unit).

Reference:

For more information, see “Unit states” (11-11).

- 2 To cold start a BSC, STU, or DTU, the unit must be standby. You can cold start an active BSC, STU, or DTU unit only if the corresponding mate is not present. Verify that the BSC, STU, or DTU is in the standby state.

Reference: For more information, see one of the following topics:

- “Querying the current status of MS Control” (9-11)
 - “Querying a DTU protection group” (9-42)
-

- 3 If you want to cold start the active BSC, STU, or DTU unit when the corresponding mate has a failure condition that you cannot clear, see “Performing a cold start when the corresponding mate has a failure” (11-44).

END OF STEPS

Procedure

- 1** Go to the Unit Control window at *Maintenance > Controller Maintenance > Unit Control*.

- 2** In the Unit ID field, select the address of the unit you want to cold start.

- 3** Select COLD in the Initialisation Level field.

Result:

If the Unit ID is a BSC, DTU, STU, or a port unit, the system gives you the option of checking the Force Reload box.

Reference:

For more information about the Force Reload box, see the field descriptions for Force Reload at “Field descriptions” (11-38).

- 4** Click Initialise.

Result:

If the request is going to affect service, the system displays a list of units affected by the service interruption and asks you to confirm this request.

The hour glass disappears from the screen about 30 seconds after the initialisation completes. If you have requested a cold start of the active DTU, transmission can still be affected for another 30 seconds after the DTU initialisation completes, because the DTU is initialising the BSIUs.

END OF STEPS



Performing a cold start when the corresponding mate has a failure

Purpose Use this procedure to cold start an active BSC, STU, or DTU when the corresponding mate has a failure condition that you cannot clear.

Procedure



CAUTION

The following step may affect service.

- 1 Force switch the unit to the standby side.

Reference: For more information, see one of the following topics:

- “Requesting an MS Control protection switch” (9-18)
 - “Requesting a DTU protection group switch” (9-49)
-

- 2 Go to the Unit Control window at *Maintenance > Controller Maintenance > Unit Control*.
-

- 3 In the Unit ID field, select the address of the unit you want to cold start.
-

- 4 Select COLD in the Initialisation Level field.

Result:

If the Unit ID is a BSC, DTU, STU, or port unit, the system gives you the option of checking the Force Reload box.

Reference:

For more information about the Force Reload box, see the field descriptions for Force Reload at “Field descriptions” (11-38).

- 5 Click Initialise.

Result:

If the request is going to affect service, the system displays a list of units affected by the service interruption and asks you to confirm this request.

The hour glass disappears from the screen about 30 seconds after the initialisation completes. If you have requested a cold start of the active DTU, transmission can still be affected for another 30 seconds after the DTU initialisation completes, because the DTU is initialising the BSIUs.

6 Switch service back to the active side.

Reference: For more information, see one of the following topics:

- “Requesting an MS Control protection switch” (9-18)
- “Requesting a DTU protection group switch” (9-49)

END OF STEPS





12 Execute equipment tests

Overview

- Purpose** “Execute equipment tests” contains the following information:
- General information about diagnostic tests
 - Descriptions of the windows that are used to run diagnostic tests
 - Step-by-step procedures for running diagnostic tests on the equipment

- Organisation** “Execute equipment tests” is organised as follows:
- “Background information” (12-2)
 - “Diagnostic Tests window” (12-17)
 - “BCLAN diagnostic tests” (12-20)
 - “DFWT diagnostic tests” (12-27)
 - “MD Inputs diagnostic test” (12-50)
 - “BSSU Optical Loopback diagnostic test” (12-55)
 - “STU Station Clock diagnostic test” (12-61)
 - “BSC, BSIU, BSSU, DTU, and STU Unit diagnostic tests” (12-67)
 - “All other equipment diagnostic tests” (12-80)
 - “Diagnostic Testing - Test Results window” (12-87)



Background information

Overview

Purpose This section contains background information about equipment diagnostic tests.

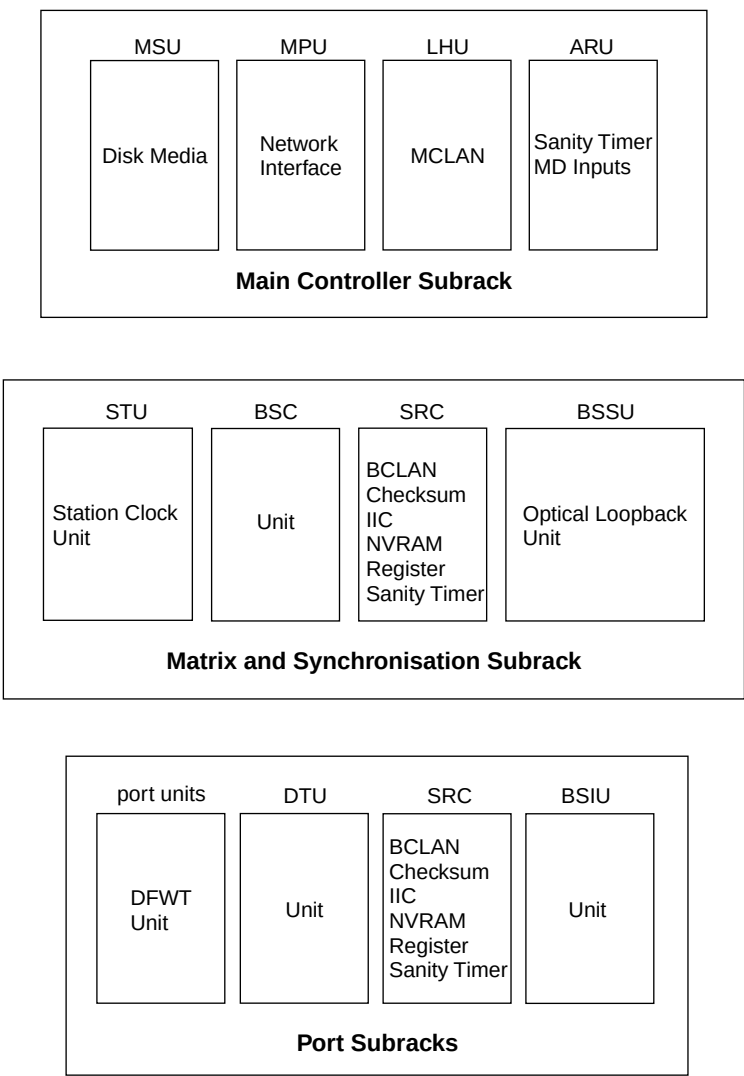
Organisation This section is organised as follows:

- [“About the tests” \(12-3\)](#)
- [“Equipment diagnostic test terms” \(12-6\)](#)
- [“Foreground and background modes” \(12-8\)](#)
- [“Where to query diagnostic test results” \(12-9\)](#)
- [“Where the system displays diagnostic test results” \(12-10\)](#)
- [“Alarms and LEDs caused by diagnostic tests” \(12-11\)](#)
- [“Protection switching and diagnostic tests” \(12-12\)](#)
- [“Special equipment for diagnostic tests” \(12-13\)](#)
- [“About running diagnostic tests on more than one subrack” \(12-14\)](#)
- [“About removing units” \(12-15\)](#)
- [“About testing cables” \(12-16\)](#)



About the tests

What tests are available? The following diagram shows the tests that are available for each unit.



Test descriptions The following is a description of each diagnostic test.

Test	Runs a diagnostic test on	Go to
BCLAN	all the working and protection units on the active BCLAN.	“BCLAN procedure” (12-21)
Checksum	the EPROMS on the SRCs.	“All other equipment diagnostic tests” (12-81)

Test	Runs a diagnostic test on	Go to
DFWT optical	the input and output optic devices in the optical port units.	See one of the following: “DFWT procedure for optical STM-1s” (12-29) “DFWT procedure for STM-4s” (12-34) “DFWT procedure for STM-16s” (12-38)
DFWT electrical	the input and output optic devices in the STM-1 electrical unit.	“DFWT procedure for electrical STM-1s” (12-44)
Disk Media	the hard drive on the MSU and the SCSI controller on the MSU.	“All other equipment diagnostic tests” (12-81)
IIC	the ability of the SRC to communicate across the IIC bus.	“All other equipment diagnostic tests” (12-81)
MCLAN	the provisioned ports of LHUs that are part of an MCLAN.	“All other equipment diagnostic tests” (12-81)
MD Inputs	the Miscellaneous Discrete Inputs circuitry on the ARU.	“MD Inputs procedure” (12-51)
Network Interface	the Network Interface Chip (NIC) devices, and the cables and connectors from the MPU’s NIC to the LHU.	“All other equipment diagnostic tests” (12-81)
NVRAM	the Real Time Clock Nonvolatile RAM.	“All other equipment diagnostic tests” (12-81)

Test	Runs a diagnostic test on	Go to
Optical Loopback	all eight Equipment Core Interface (ECI) optical transceivers on the BSSU unit.	“BSSU Optical Loopback procedure” (12-56)
Register Test	the backplane connectivity on the SRCs.	“All other equipment diagnostic tests” (12-81)
Sanity Timer	the sanity timer circuitry on the ARU and SRC.	“All other equipment diagnostic tests” (12-81)
Station Clock	the ability of the STU to properly detect and phaselock to the station clock input signals.	“STU Station Clock procedure” (12-62)
Unit – BSC	the internal hardware on the BSC unit.	“BSC Unit procedure” (12-68)
Unit – BSIU	the internal hardware on the BSIU.	“BSIU and BSSU Unit procedure ” (12-71)
Unit – BSSU	the internal hardware on the BSSU.	“BSIU and BSSU Unit procedure ” (12-71)
Unit – DTU	the internal hardware on the DTU.	“DTU Unit procedure” (12-74)
Unit – port	the internal hardware on the STM-1, STM-4, or STM-16.	“All other equipment diagnostic tests” (12-81)
Unit – STU	the internal hardware on the STU.	“STU Unit procedure” (12-77)



Equipment diagnostic test terms

- List of terms**
- Background test** An equipment diagnostic test is in background test mode when 2-6 diagnostic tests are running at the same time, and more than one unit is being tested. You can perform other tasks from the terminal while the system is executing tests in background mode.
- BCLAN** The Board Controller Local Area Network (BCLAN) is an internal local area network that provides communications between the line and board controllers on the units associated with a high-speed line.
- Diagnostic test** Tests the internal hardware on a unit.
- Errored** When a diagnostic test displays an errored message, it means that the system could not complete a diagnostic test.
- External tests** External diagnostic tests require you to install external equipment. This external equipment can be loopback cables, a splitter, or an adapter. The following tests are external:
- DFWT — optical port units
 - DFWT — STM-1 electrical
 - MD Inputs — ARU
 - Optical Loopback — BSSU
 - Station Clock — STU
- Failed** When a diagnostic test displays a failed message, it means that the equipment did not pass a diagnostic test.
- Foreground test** An equipment diagnostic test is in foreground test mode when only one diagnostic test is running on the system, and only one unit is being tested. You *cannot* perform other tasks from the terminal while the system is executing a test in foreground mode.
- Internal tests** Internal diagnostic tests do *not* require you to install special equipment to perform the diagnostic test.
- Network Interface Chip (NIC)** A Network Interface Chip (NIC) is a DEC 21140-A device capable of both 10BaseT or 100BaseT operations.
- Partial Passed** When a diagnostic test displays a Partial Passed message, it means that the system tested and passed all the equipment *available* for the test in the current configuration. The screen will display this result if one or more units that could have been tested were not present, and therefore, were not tested.
- Passed** When a diagnostic test displays a passed message, it

means that the system tested all the equipment available for the test, and all of the equipment passed the diagnostic test.



Foreground and background modes

Differences between foreground and background modes

Diagnostic tests can run in either foreground or background mode. The type of diagnostic tests that can run in the background are the same as those that can run in the foreground. Foreground and background diagnostic tests have the following characteristics.

Foreground mode	Background mode
You can run one diagnostic test at a time.	You can run up to six diagnostic tests at a time.
You can test only one unit.	You can test one or more units.
The screen waits for the diagnostic test to complete.	The screen does not wait for the diagnostic test to complete.
You cannot perform other tasks on the terminal while the diagnostic test is running.	You can perform other tasks on the terminal while the diagnostic tests are running.
You can run a diagnostic test one time.	You can run a diagnostic test one or more times.

How to run a test in foreground or background mode

- To run a diagnostic test in the background, do one or more of the following from the Diagnostic Tests window:
- Select ALL anywhere in the Unit ID, Test Type, or Test subfields or fields.
 - Select a number greater than 1 in the Loop Count field.
 - Check the Background Test box.

If you do none of these things, the diagnostic test will run in foreground mode.



Where to query diagnostic test results

Diagnostic tests query table

You cannot request queries from the Diagnostic Tests window and see a query results screen as in most windows. Use the following table to decide how to best perform a query on diagnostic tests.

To query	Do the following
Background tests in progress	Use the Background Tests window
A test that has completed	Use the View Test Results window
The details (the 64-byte field) of a test that has completed and failed	Run the test again in the foreground using the Diagnostic Tests window

Related topics

For more information, see one of the following topics:

- “Displaying background tests in progress” (15-4)
- “How to view completed test results” (14-3)



Where the system displays diagnostic test results

Diagnostic tests display table

Where the system displays the results or status of a diagnostic test depends on whether the test is run in the foreground or in the background, and whether the test is in progress or has completed.

Type of diagnostic test	Where it is displayed or viewed
The results of a foreground test	The system automatically displays the results from the Diagnostic Tests window after the test completes
The results of completed background tests	The View Test Results window
The status of in-progress background tests	The Background Tests window

- Related topics**
- For more information, see one of the following topics:
- “Displaying background tests in progress” (15-4)
 - “How to view completed test results” (14-3)



Alarms and LEDs caused by diagnostic tests

Alarms caused when a test passes

In some cases, even if a diagnostic test passes, the diagnostic test may temporarily cause equipment alarms and light LEDs on units other than the unit being tested. All alarms and LEDs lit by the diagnostic test will return to normal after 1 or 2 minutes.

Alarms caused when a test fails

If the diagnostic test fails, the diagnostic test will generate an equipment alarm. The alarm will be raised against the unit tested, not necessarily against the defective hardware.

How to clear an alarm generated by a diagnostic test

There are three ways to clear an alarm generated by a diagnostic test:

- Install a new unit or reseal the same unit.
- Restart the SRC.
- Run the same diagnostic test on the unit until the diagnostic test passes.

Related topic

For more information, see “Restoring an SRC to service” (11-35).

LEDs lit by diagnostic tests

For units with red LEDs, all of the diagnostic tests will cause the red LED to light on the affected equipment.



Protection switching and diagnostic tests

About running diagnostic tests on active units

Whenever possible, run diagnostic tests on standby units. Running a service-affecting diagnostic test on an active unit may temporarily disconnect the cross connect.

Units that must be in the standby protection-switch state

The system will not allow you to run a BSSU, DTU, BSC, or STU Unit diagnostic test unless the unit, or the subrack housing the unit, is in the standby state. The system requires the unit to be in the standby state to prevent the system from automatically switching to the protection state while the diagnostic test is in progress.

Related topics

For more information, see one of the following topics:

- Chapter 9, “Equipment protection switching”
- “BSIU and BSSU Unit procedure” (12-71)
- “DTU Unit procedure” (12-74)
- “BSC Unit procedure” (12-68)
- “STU Unit procedure” (12-77)

Protection switching caused by a failed diagnostic test

After a failed diagnostic test, the system may cause a protection switch to occur based on the following criteria:

- The system can isolate the fault to a particular unit.
- The fault is service affecting.
- The current state of the system will allow the protection switch to occur.

Protection state changes caused by diagnostic tests

If you run a diagnostic test on a unit that is part of a protection group, the diagnostic test can change the protection state of any units in the affected protection group to Clear from any of the following:

- Freeze
- Force Switch to Protect
- Force Switch to Working

Switch the unit back to its original state after the diagnostic test has completed.



Special equipment for diagnostic tests

External tests Special equipment is required for some diagnostic tests. Diagnostic tests that require looparound cables, a splitter, or an adapter are known as external diagnostic tests.

The following diagnostic tests are the only tests that require special equipment.

Test	Unit tested	Required equipment
DFWT	STM-1 optical using IM01 or IM05 interface units	Four SC/SC optical cables for each STM-1 unit tested
DFWT	STM-1 optical using an IM09 interface unit	Eight LC/SC optical cables, four 10–20 dB attenuators, and four couplers for each STM-1 tested
DFWT	STM-4	Four LC/LC optical cables for each STM-4 tested
DFWT	STM-16	Two LC/SC optical cables, one 10–20 dB attenuator, and one coupler for each STM-16 tested
DFWT	STM-1 electrical	Four 75-ohm BNC cables for each STM-1 tested
MD Inputs	ARU	One MD Input Loopback Adapter
Optical Loopback	BSSU	One SC/SC optical cable for each spare port
Station Clock	STU	One RF splitter (ZFSC-2-1-75-6)

Related topic

For more information about attenuators, see “How to install an attenuator” (12-28).



About running diagnostic tests on more than one subrack

Preferred order Do *not* run a diagnostic test on more than one subrack at a time. It is especially important not to run diagnostic tests on the Matrix/Synchronisation and port subracks at the same time. The best way to run diagnostic tests is on one subrack at a time in the following order:

1. Units on the Main Controller subrack
2. Units on the Matrix and Synchronisation subrack
3. Units on a port subrack



About removing units

Removing units prior to and during diagnostic tests

Consider the following when you remove a unit:

- If you remove a unit during a diagnostic test, the test will time out.
- If you remove a unit prior to a diagnostic test, the test will return a system message.



About testing cables

Self-supervised cables There is no need to run a diagnostic test on a cable. The cables on this system are self-supervised, meaning that the system automatically monitors the cables and generates an alarm when the system discovers a problem.

Related topics For more information, see one of the following topics:

- “Fibre addresses” (5-19)
- “About internal fibre connections” (3-5)
- “CABLEcEQ description” (21-22)
- “CABLEcTIM description” (21-27)
- “INTFcEQ description” (21-109)



Diagnostic Tests window

Overview

Purpose This section provides information about the Diagnostic Tests window.

Window location *Maintenance > Execute Tests > Diagnostic Tests*

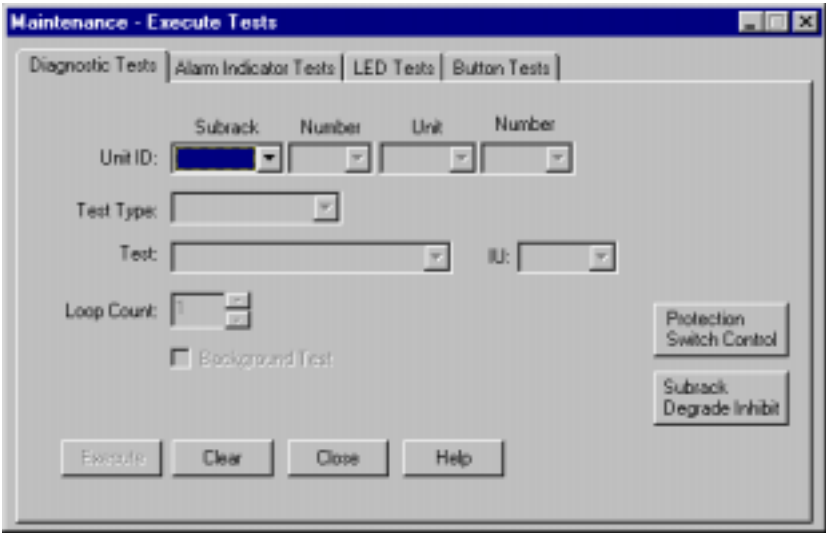
Organisation This section is organised as follows:

- [“BCLAN diagnostic tests” \(12-20\)](#)
- [“DFWT diagnostic tests” \(12-27\)](#)
- [“MD Inputs diagnostic test” \(12-50\)](#)
- [“BSSU Optical Loopback diagnostic test” \(12-55\)](#)
- [“STU Station Clock diagnostic test” \(12-61\)](#)
- [“BSC, BSIU, BSSU, DTU, and STU Unit diagnostic tests” \(12-67\)](#)
- [“All other equipment diagnostic tests” \(12-80\)](#)



Diagnostic Tests window description

Illustration The following illustration shows the Diagnostic Tests window.



Field descriptions The Diagnostic Tests window has the following fields.

Field name	Description
Unit ID	The Unit ID field specifies the physical location of the unit that you want tested. For a description of the Unit IDs, see “About physical layer addresses” (5-3).
Test Type	The Test Type field specifies the type of diagnostic test as one of the following: • Internal — tests that do not require external cable connections • External — tests that require external cable connections • All — both internal and external tests
Test	The Test field specifies the diagnostic test you want to run. For a list of tests, see “Test descriptions” (12-3).
IU	The IU field allows you to specify the address of the interface unit that is associated with an STM-1 unit. Use this field when running DFWT tests on either the STM1-9 or STM1-19. The Unit ID specifies the STM-1 protection unit and the IU field specifies the Interface Unit.

Field name	Description
Loop Count	The Loop Count field specifies the number of times (1-25) the system repeats a diagnostic test. The default value is 1.
Background Test	A check in this box will tell the system to run a <i>single</i> test in the background. This field was designed for factory personnel. All other users will probably find this feature unnecessary.
Protection Switch Control	Before running certain diagnostic tests, you will first need to query the protection state and perform a protection switch. This button will connect you to the Matrix Control window.
Subrack Degrade Inhibit	You may want to perform a subrack degrade inhibit before running certain diagnostic tests. This button will connect you to the Subrack window where this feature is located.

Related topic For general information about windows, see “About the main application window” (4-10).



BCLAN diagnostic tests

Overview

Purpose This section contains information about the BCLAN diagnostic test.

Organisation This section is organised as follows:

- “BCLAN procedure” (12-21)
- “How to interpret BCLAN failure results” (12-23)
- “What to do if the BCLAN diagnostic test fails” (12-26)



BCLAN procedure

Purpose The BCLAN diagnostic test will test all the working and protection units on the active BCLAN. Then the system will perform a protection switch to the standby BCLAN and test those units. If the diagnostic test passes, the system will **not** switch service back to the originally-active BCLAN. If you started the test with the working LAN active, the protection LAN will be active after the test, and vice-versa.

What units are tested The following procedure will test both the working and protection BCLANs for all the units in the subrack that are connected to the LAN.

Subrack	Units tested
MS	STU, BSC
port	all port units, both DTUs

Procedure overview The following list describes the procedures required for a BCLAN diagnostic test:

- “Gathering information” (12-21)
- “Running a BCLAN diagnostic test” (12-22)
- “How to interpret BCLAN failure results” (12-23)
- “What to do if the BCLAN diagnostic test fails” (12-26)

Gathering information Do the following before running a BCLAN diagnostic test.

- 1 To save yourself time and possible service interruption, read “Background information” (12-2).
- 2 Query the unit at *Provision > Equipment > Unit*. Verify that the unit you are testing displays *Unit provisioned and initialised* in the Unit Status field.
- 3 Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes.

END OF STEPS

Running a BCLAN diagnostic test

- 1 Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.

- 2 Select the address of the BCLAN you want to test in the Unit ID field.

Result:

The system automatically populates the Test Type field as Internal.

- 3 Select BCLAN in the Test field.

- 4 If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected ALL in the Unit ID field, or if you specified a number greater than 1 in the Loop Count field.

- 5 Click Execute.

END OF STEPS

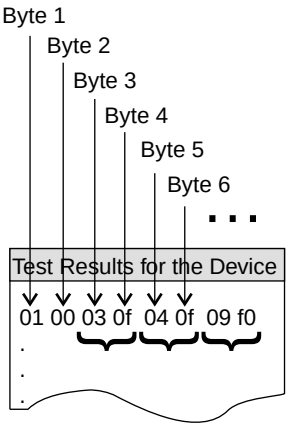
Related topics If the test failed, see one of the following:

- “How to interpret BCLAN failure results” (12-23)
- “What to do if the BCLAN diagnostic test fails” (12-26)



How to interpret BCLAN failure results

Byte positions If the BCLAN test fails, the Test Results for the Device column on the Diagnostic Testing - Test Results window will provide information about why the test failed.



The pairs that are grouped within the braces in the diagram are interpreted together. The number of byte pairs populated with information depends on how many units in the LAN failed or errored the diagnostic test.

Byte meanings The bytes in the Test Results for the Device column contain the following information.

Byte	Description
1	The following list describes the meaning of byte 1: • 00 = passed • 01 = failed • 02 = errored • 03 = partial passed
2	Byte 2 describes which LAN was left active, working (00) or protection (01).
3	Byte 3 displays a code for the first unit that failed or errored. To interpret the codes, see one of the following: • “Which unit on the MS subrack failed or errored?” (12-24) • “Which unit on a port subrack failed or errored?” (12-24)

Byte	Description
4	Bytes 3 and 4 are interpreted together. Byte 4 describes which LAN the failed or errored unit is on. For a description of the codes that may appear in byte 4, see “Which LAN failed or errored?” (12-25)
5	Byte 5 displays a code for the second unit that failed or errored, if a second unit failed or errored.
6	Bytes 5 and 6 are interpreted together. Byte 6 refers to the LAN of the unit that failed or errored in byte 5.

Pairs of codes are displayed in subsequent bytes if more units failed or errored the test.

Which unit on the MS subrack failed or errored?

Use the following table to help you determine which unit on the Matrix and Synchronisation subrack failed or errored the BCLAN diagnostic test. The value in the first column describes the values that appear in bytes 3, 5, 7, et cetera.

Value in byte 3, 5, 7, ...	Unit on MS subrack
01	BSC-1
05	STU-1

Which unit on a port subrack failed or errored?

Use the following table to help you determine which unit on a port subrack failed or errored the BCLAN diagnostic test. The value in the first column describes the values that appear in bytes 3, 5, 7, et cetera.

Value in byte 3, 5, 7, ...	Port unit
01	STM{1, 4, 16}-1
02	STM{1, 4, 16}-2
03	STM{1, 4, 16}-3
04	STM{1, 4, 16}-4
05	STM{1, 4, 16}-5
06	STM{1, 4, 16}-6
07	STM{1, 4, 16}-7
08	STM{1, 4, 16}-8
09	STM1-9
0a	DTU-1
0c	STM1-11
0d	STM1-12

Value in byte 3, 5, 7, ...	Port unit
0e	STM1-13
0f	STM1-14
10	STM1-15
11	STM1-16
12	STM1-17
13	STM1-18
14	STM1-19
15	DTU-2

Which LAN failed or errored?

Use the following table to help you determine which LAN failed or errored the diagnostic test. The value in the first column describes the values that appear in bytes 4, 6, 8, et cetera.

Value in byte 4, 6, 8 ...	Description
ef	Working LAN errored, protection LAN failed
fe	Working LAN failed, protection LAN errored
f0	Working LAN failed, protection LAN passed
0f	Working LAN passed, protection LAN failed
ff	Working LAN failed, protection LAN failed
77	The unit is in the wrong state. It is either in maintenance or booting.



What to do if the BCLAN diagnostic test fails

Procedure

- 1 Replace the unit identified as defective in the test.

Reference: For more information, see one of the following:

- “How to interpret BCLAN failure results” (12-23)
 - “FLTcEQ flowcharts and procedures” (21-48)
-

- 2 Repeat the diagnostic test.
-

- 3 If the diagnostic test fails again, replace the SRC.

Reference:

For more information, see “Clearing a FLTcEQ on an SRC” (21-75).

- 4 Repeat the diagnostic test.
-

- 5 If the diagnostic test fails again, record the date and time this occurred, and call technical support.

END OF STEPS



DFWT diagnostic tests

Overview

Purpose This section contains information about the Distributed Frame Wiring Test (DFWT) diagnostic tests.

Organisation This section is organised as follows:

- [“How to install an attenuator” \(12-28\)](#)
- [“DFWT procedure for optical STM-1s” \(12-29\)](#)
- [“DFWT procedure for STM-4s” \(12-34\)](#)
- [“DFWT procedure for STM-16s” \(12-38\)](#)
- [“What to do if a DFWT fails on an optical port unit” \(12-42\)](#)
- [“DFWT procedure for electrical STM-1s” \(12-44\)](#)
- [“How to interpret which electrical STM-1 IU failed” \(12-48\)](#)
- [“What to do if a DFWT fails on an electrical STM-1” \(12-49\)](#)



How to install an attenuator

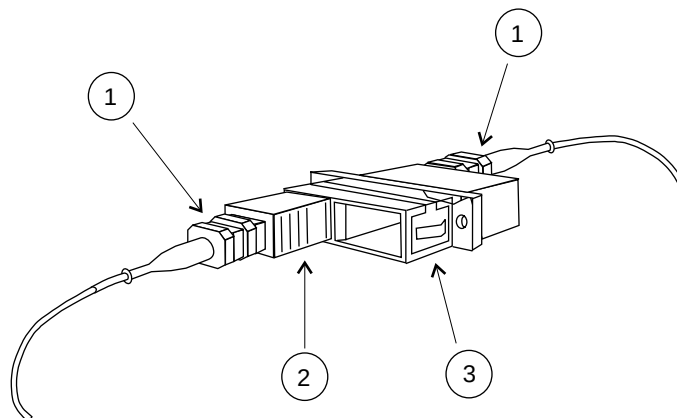
Purpose Use an attenuator if you are running a DFWT diagnostic test on an STM-1 optical unit that has an IM09 Interface Unit (IU), or an STM-16 unit. You must install one attenuator for *each* looparound.

Equipment required For *each* looparound you install, you will need the following equipment:

- Two LC/SC cables for an STM-16
- Eight LC/SC cables for an STM-1 with an IM09 IU
- One attenuator
- One coupler

Lucent Technologies does not manufacture attenuators. You must obtain attenuators from companies that manufacture them.

Installation diagram Install the attenuator in the loopback as described in this diagram.



Legend:

1. SC connection side of cable
2. Attenuator
3. Coupler



DFWT procedure for optical STM-1s

Purpose	The DFWT optical STM-1 unit diagnostic test, tests the input and output optic devices in the STM-1 optical port units.
Procedure overview	The following list describes the procedures required for a DFWT optical STM-1 unit diagnostic test: • “Gathering information” (12-29) • Choose one of the following: - “Setting up looparounds for optical STM-1s with IM01 or IM05 IUs” (12-30) - “Setting up looparounds for optical STM-1s with IM09 IUs” (12-31) • “Running a DFWT optical STM-1 diagnostic test” (12-32) • “What to do if a DFWT fails on an optical port unit” (12-42)
Gathering information	Do the following before running a DFWT optical diagnostic test. 1 To save yourself time and possible service interruption, read “Background information” (12-2). 2 Query the unit at <i>Provision > Equipment > Unit</i>. Verify that the unit you are testing displays <i>Unit provisioned and initialised</i> in the Unit Status field. 3 Use the same Unit window to verify that there is at least one DTU in the subrack. 4 Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes. END OF STEPS

**Setting up looparounds
for optical STM-1s with
IM01 or IM05 IUs**

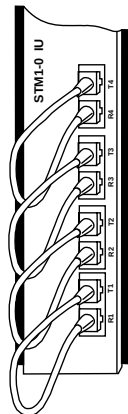
Use this procedure only if the STM-1 unit you are testing has IM01 or IM05 Interface Units (IUs).

- 1 Obtain four SC/SC optical cables for *every* STM-1 unit that you will test.

Example:

If you are running a test on two units simultaneously, you will need eight optical cables.

- 2 Locate the connectors on the IU associated with the port unit by going to the rear of the port subrack.
- 3 On the IU, remove all connector covers.
- 4 Install the looparound cables in the unit connectors R1 to T1, R2 to T2, R3 to T3, and R4 to T4.



- 5 If you want to test more than one port unit, install looparound cables for the other port units.

END OF STEPS

**Setting up looparounds
for optical STM-1s with
IM09 IUs**

Use this procedure only if the STM-1 unit you are testing has IM09 Interface Units (IUs).

- 1 Obtain the required equipment to run this test.

Reference:

For more information, see “How to install an attenuator” (12-28).

- 2 Locate the connectors on the IU associated with the STM-1 unit by going to the rear of the PSA subrack.

- 3 On the IU, remove all connector covers.



CAUTION

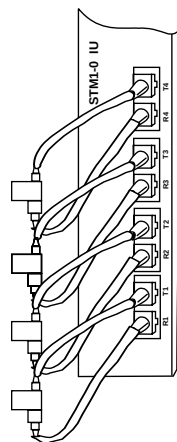
Failure to use a 10–20 dB attenuator for each looparound could damage an analyser or the receiver on a unit.

- 4 Install an attenuator in each loopback.

Reference:

For more information about attenuators, see “How to install an attenuator” (12-28).

- 5 Install the assembled looparounds in the unit connectors R1 to T1, R2 to T2, R3 to T3, and R4 to T4.



-
- 6 If you want to test more than one STM-1 unit, install looparounds for the other STM-1 units.

END OF STEPS

Running a DFWT optical STM-1 diagnostic test

- 1 Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.
-

- 2 Select the appropriate address for the STM-1 unit in the Unit ID field.
If you want to run a test on all STM-1 units, select ALL (for example: PSA-4-STM1-ALL).
-

- 3 Select External in the Test Type field.

Result:

The system automatically populates the Test field as DFWT.

- 4 If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected ALL in the Unit ID field, or if you specified a number greater than 1 in the Loop Count field.

- 5 Click Execute.

Result:

Since the test is service affecting, the system asks you to confirm the command.

- 6 Click yes.

Result:

If you ran the test in the foreground, the system displays the results of the diagnostic test on the screen.

- 7 Remove the looparound cables.

END OF STEPS

Related topic If the diagnostic test failed, see “What to do if a DFWT fails on an optical port unit” (12-42).



DFWT procedure for STM-4s

Purpose The DFWT optical STM-4 unit diagnostic test, tests the input and output optic devices in the STM-4 optical port units.

Procedure overview The following list describes the procedures required for a DFWT optical STM-4 unit diagnostic test:

- “Gathering information” (12-34)
- “Setting up looparounds for STM-4s” (12-35)
- “What to do if a DFWT fails on an optical port unit” (12-42)

Gathering information Do the following before running a DFWT diagnostic test.

- 1** To save yourself time and possible service interruption, read “Background information” (12-2).

- 2** Query the unit at *Provision > Equipment > Unit*. Verify that the unit you are testing displays Unit provisioned and initialised in the Unit Status field.

- 3** Use the same Unit window to verify that there is at least one DTU in the subrack.

- 4** Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes.

END OF STEPS

Setting up looparounds for STM-4s

- 1 Obtain four LC/LC optical cables for *every* STM-4 unit that you will test.

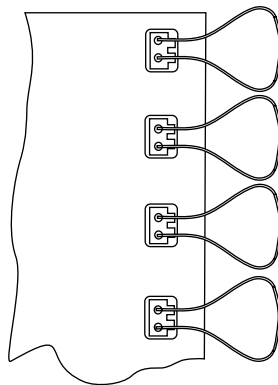
Example:

If you are running a test on two units simultaneously, you will need eight optical cables.

- 2 Go to the rear of the PSC subrack and locate the optical interconnection panel that is located behind the STM-4 units.

- 3 Locate the connectors for the STM-4 you want to test.

- 4 Install the looparounds in the unit connectors 1 T to R, 2 T to R, 3 T to R, and 4 T to R.



- 5 If you want to test more than one STM-4 unit, install looparounds for the other STM-4 units.

END OF STEPS

Running a DFWT STM-4 diagnostic test

- 1 Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.

- 2 Select the appropriate address for the STM-4 unit in the Unit ID field.
If you want to run a test on all STM-4 units, select ALL (for example: PSC-4-STM4-ALL).

- 3 Select External in the Test Type field.

Result:

The system automatically populates the Test field as DFWT.

- 4 If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected ALL in the Unit ID field, or if you specified a number greater than 1 in the Loop Count field.

- 5 Click Execute.

Result:

Since the test is service affecting, the system asks you to confirm the command.

- 6 Click yes.

Result:

If you ran the test in the foreground, the system displays the results of the diagnostic test on the screen.

- 7 Remove the looparound cables.

END OF STEPS

Related topic If the diagnostic test failed, see “What to do if a DFWT fails on an optical port unit” (12-42). □

DFWT procedure for STM-16s

Purpose The DFWT optical STM-16 unit diagnostic test tests the input and output optic devices in the STM-16 optical port units.

Procedure overview The following list describes the procedures required for a DFWT optical STM-16 unit diagnostic test:

- “Gathering information” (12-38)
- “Setting up looparounds for STM-16s” (12-39)
- “What to do if a DFWT fails on an optical port unit” (12-42)

Gathering information Do the following before running a DFWT diagnostic test.

- 1** To save yourself time and possible service interruption, read “Background information” (12-2).
- 2** Query the unit at *Provision > Equipment > Unit*. Verify that the unit you are testing displays Unit provisioned and initialised in the Unit Status field.
- 3** Use the same Unit window to verify that there is at least one DTU in the subrack.
- 4** Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes.

END OF STEPS

Setting up looparounds for STM-16s

- 1 Obtain the required equipment to run this test.

Reference:

For more information, see “How to install an attenuator” (12-28).

- 2 Go to the rear of the PSC subrack, and locate the optical interconnection panel that is located behind the STM-16 units.
-

- 3 Locate the connectors for the STM-16 you want to test.
-



CAUTION

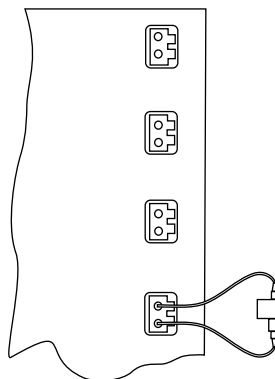
Failure to use a 10–20 dB attenuator for the looparound could damage an analyser or the receiver on a unit.

- 4 Install an attenuator in the loopback.

Reference:

For more information about attenuators, see “How to install an attenuator” (12-28).

- 5 Install the assembled looparound in the *bottom* unit connectors 1 T to R.



- 6 If you want to test more than one STM-16 unit, install assembled looparounds for the other STM-16 units.

END OF STEPS

Running a DFWT STM-16 diagnostic test

- 1 Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.

- 2 Select the appropriate address for the STM-16 unit in the Unit ID field.

If you want to run a test on all STM-16 units, select ALL (for example: PSC-4-STM16-ALL).

- 3 Select External in the Test Type field.

Result:

The system automatically populates the Test field as DFWT.

- 4 If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected ALL in the Unit ID field, or if you specified a number greater than 1 in the Loop Count field.

- 5 Click Execute.

Result:

Since the test is service affecting, the system asks you to confirm the command.

- 6 Click yes.

Result:

If you ran the test in the foreground, the system displays the results of the diagnostic test on the screen.

- 7 Remove the looparound cables.

END OF STEPS

Related topic If the diagnostic test failed, see “What to do if a DFWT fails on an optical port unit” (12-42).



What to do if a DFWT fails on an optical port unit

Procedure

- 1 Verify that the optical port units that failed have looparound cables connected to the correct ports.

Reference: For more information, see one of the following topics:

- “Setting up looparounds for optical STM-1s with IM01 or IM05 IUs” (12-30)
 - “Setting up looparounds for optical STM-1s with IM09 IUs” (12-31)
 - “Setting up looparounds for STM-4s” (12-35)
 - “Setting up looparounds for STM-16s” (12-39)
-

- 2 Repeat the diagnostic test.
-

- 3 If the diagnostic test fails again, install new looparound cables.
-

- 4 Repeat the diagnostic test.
-

- 5 If the diagnostic test fails again, replace the IU unit.

Reference:

For the appropriate unit-replacement procedure, see “Clearing a FLTcEQ on an IU or an unprotected port unit” (21-67).

- 6 Repeat the diagnostic test.
-

- 7 If the diagnostic test fails again, replace the port unit.

Reference: For the appropriate unit-replacement procedure, see one of the following topics:

- “Clearing a FLTcEQ on an IU or an unprotected port unit” (21-67)
 - “Clearing a FLTcEQ on a port unit that uses NTT MSP” (21-81)
 - “Clearing a FLTcEQ on a port unit that uses SNCP, ITU MSP, or ANSI MSP” (21-85)
-

What to do if a DFWT fails on an optical
port unit

.....
8 Repeat the diagnostic test.

.....
9 If the diagnostic test fails again, record the time and date this
occurred, and call technical support.

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



DFWT procedure for electrical STM-1s

Purpose The DFWT tests the input and output optic devices in the STM-1 electrical unit. If the unit under test is a working unit, the system will check the signal path to the external connectors through the Interface Unit (IU). If the unit is a protection unit, the system will check the signal path from the protection unit to a specific IU.

Procedure overview The following list describes the procedures required for a DFWT STM-1 electrical diagnostic test:

- “Gathering information” (12-44)
- “Setting up looparounds for electrical STM-1s” (12-45)
- “Running a DFWT electrical STM-1 diagnostic test” (12-46)
- “How to interpret which electrical STM-1 IU failed” (12-48)
- “What to do if a DFWT fails on an electrical STM-1” (12-49)

Gathering information Do the following before running a DFWT STM-1 electrical diagnostic test.

- 1** To save yourself time and possible service interruption, read “Background information” (12-2).

- 2** Query the unit at *Provision > Equipment > Unit*. Verify that the unit you are testing displays Unit provisioned and initialised in the Unit Status field.

- 3** Use the same Unit window to verify that there is at least one DTU in the subrack.

- 4** Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes.

- 5** Query the protection status of the working or protection unit you are testing to verify that the unit is active. The system will not allow you to run a DFWT electrical test on a standby unit because the test will not have access to the associated Interface Unit (IU) when it is in standby.

Reference:

Use the STM1 1:8 window at *Protection > Equipment > STM1 1:8*.

END OF STEPS

**Setting up looparounds
for electrical STM-1s**

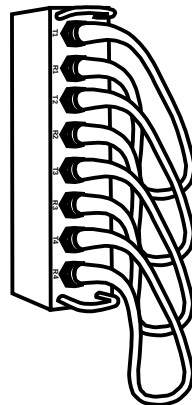
- 1 Obtain four 75-ohm BNC cables for *every* STM-1 unit that you will test.

Example:

If you are running a test on 3 units simultaneously, you will need 12 cables.

- 2 Locate the connectors on the back of the STM-1 unit by going to the rear of the PSA subrack.
-

- 3 Install the four looparound cables in the unit connectors as follows:
 - R1 to T1
 - R2 to T2
 - R3 to T3
 - R4 to T4



- 4 If you want to test more than one STM-1 unit, also install looparound cables for the other STM-1 units.

END OF STEPS

Running a DFWT electrical STM-1 diagnostic test

- 1 Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.

- 2 Select the ID of the unit or units you want to test in the Unit ID field.

- 3 Select External in the Test Type field.

Result:

The system automatically populates the Test field as DFWT.

- 4 Select the Interface Unit address in the IU field as one of the following:

- 1–8 for STM1-9
- 11–18 for STM1-19

If you select 9 or 19 in the Unit ID field, the system will require an IU address.

- 5 If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected ALL in the Unit ID field, or if you selected a number greater than 1 in the Loop Count field.

- 6 Click Execute.

Result:

Since the test is service affecting, the system asks you to confirm the command.

- 7 Click yes.

Result:

If you ran the test in the foreground, the system displays the results of the diagnostic test on the screen.

- 8 Remove the looparound cables.

END OF STEPS

Related topics If the test failed, see one of the following topics:

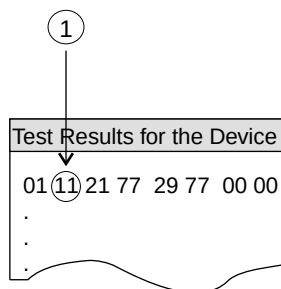
- “How to interpret which electrical STM-1 IU failed” (12-48)
- “What to do if a DFWT fails on an electrical STM-1” (12-49)



How to interpret which electrical STM-1 IU failed

How to interpret the bytes

If the DFWT electrical STM-1 diagnostic test fails, byte 2 in the Test Results for the Device column on the Diagnostic Testing - Test Results window will tell you which Interface Unit (IU) number (1–8, 11–18) failed the diagnostic test.



Legend:

1. IU that failed the DFWT electrical STM-1 test (1–8, 11–18)

DFWT test on a protection unit

The IU number displays in the Test Results for the Device column only if the DFWT test ran on the *protection* STM-1 unit.



What to do if a DFWT fails on an electrical STM-1

Procedure

- 1 Verify that the STM-1 ports that failed have looparound cables connected to the correct ports.

Reference:

For more information, see “Setting up looparounds for electrical STM-1s” (12-45).

- 2 Repeat the diagnostic test.

- 3 If the diagnostic test fails again, install new looparound cables.

- 4 Repeat the diagnostic test.

- 5 If the diagnostic test fails again, replace the IU unit.

Reference:

For the appropriate unit-replacement procedure, see “Clearing a FLTcEQ on an IU or an unprotected port unit” (21-67).

- 6 Repeat the diagnostic test.

- 7 If the diagnostic test fails again, replace the STM-1 unit.

Reference: For the appropriate unit-replacement procedure, see one of the following topics:

- “Clearing a FLTcEQ on an IU or an unprotected port unit” (21-67)
- “Clearing a FLTcEQ on an STM-1 electrical unit that uses 1:8 equipment protection” (21-77)

- 8 Repeat the diagnostic test.

- 9 If the diagnostic test fails again, record the time and date this occurred, and call technical support.

END OF STEPS



MD Inputs diagnostic test

Overview

Purpose This section contains information about the MD Inputs diagnostic test.

Organisation This section is organised as follows:

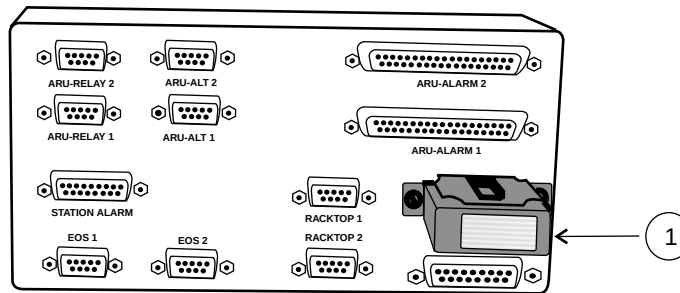
- “MD Inputs procedure” (12-51)
- “What to do if the MD Inputs diagnostic test fails” (12-54)



MD Inputs procedure

Purpose	The MD Inputs diagnostic tests the Miscellaneous Discrete Inputs circuitry on the ARU.
Procedure overview	The following list describes the procedures required for an MD Inputs diagnostic test: • “Gathering information” (12-51) • “Inserting the adapter” (12-51) • “Running an MD Inputs diagnostic test” (12-52) • “What to do if the MD Inputs diagnostic test fails” (12-54)
Gathering information	Do the following before running an MD Inputs diagnostic test. 1 To save yourself time and possible service interruption, read “Background information” (12-2). 2 Query the unit at <i>Provision > Equipment > Unit</i>. Verify that the unit you are testing displays Unit provisioned and initialised in the Unit Status field. 3 Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes. END OF STEPS
Inserting the adapter	1 Go to the Alarm Connector Panel (ACP). Reference: The ACP is located on the back of the User Panel.

- 2 Insert the MD Input Loopback Adapter into the MISC DISCRETES connector.



Legend:

1. MD Input Loopback Adapter inserted into the MISC DISCRETES connector

END OF STEPS

Running an MD Inputs diagnostic test

- 1 Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.
- 2 Select the Unit ID address.
- 3 Select External in the Test Type field.

Result:

The system automatically populates the Test field as MD Inputs and the Loop Count field as 1.

- 4 If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected a number greater than 1 in the Loop Count field.

- 5 Click Execute.

Result:

If you ran the test in the foreground, the system displays the results of the diagnostic test on the screen.

Reference:

If the test failed or errored, see “Diagnostic Testing - Test Results window” (12-87).

.....

6 Remove the adapter.

END OF STEPS

.....

Related topic If the diagnostic test failed, see “What to do if the MD Inputs diagnostic test fails” (12-54).



What to do if the MD Inputs diagnostic test fails

Procedure

- 1 Verify that the MD Inputs Loopback Adapter is connected to the MISC DISCRETES connector on the Alarm Connector Panel (ACP).

Reference:

For a diagram, see “Inserting the adapter” (12-51).

- 2 Repeat the test.
-

- 3 If the test fails again, replace the MD Inputs Loopback Adapter.
-

- 4 Repeat the test.
-

- 5 If the test fails again, replace the adapter between the MISC DISCRETES connector and the ARU.
-

- 6 Repeat the test.
-

- 7 If the test fails again, replace the ARU.

Reference:

For the ARU pack-replacement procedure, see “Clearing a FLTcEQ on an ARU, LHU, or PSP” (21-51).

- 8 Repeat the test.
-

- 9 If the diagnostic test fails again, record the time and date this occurred, and call technical support.

END OF STEPS



BSSU Optical Loopback diagnostic test

Overview

Purpose This section contains information about the BSSU Optical Loopback diagnostic test.

Organisation This section is organised as follows:

- “BSSU Optical Loopback procedure” (12-56)
- “What to do if the Optical Loopback diagnostic test fails” (12-60)



BSSU Optical Loopback procedure

Purpose The BSSU Optical Loopback diagnostic tests all eight Equipment Core Interface (ECI) optical transceivers on the BSSU unit.

Procedure overview The following list describes the procedures required for an Optical Loopback diagnostic test:

- “Gathering information” (12-56)
- “Setting up looparound cables” (12-57)
- “Running an Optical Loopback diagnostic test” (12-58)
- If the test failed or errored, see “What to do if the Optical Loopback diagnostic test fails” (12-60).
- For a description of the columns in the Diagnostic Testing - Test Results window, see “Diagnostic Testing - Test Results window” (12-87).
- For a specific description of the Test Results for the Device column, see “Test Results for the Device column description” (12-89).

Gathering information Do the following before running a BSSU Optical Loopback diagnostic test.

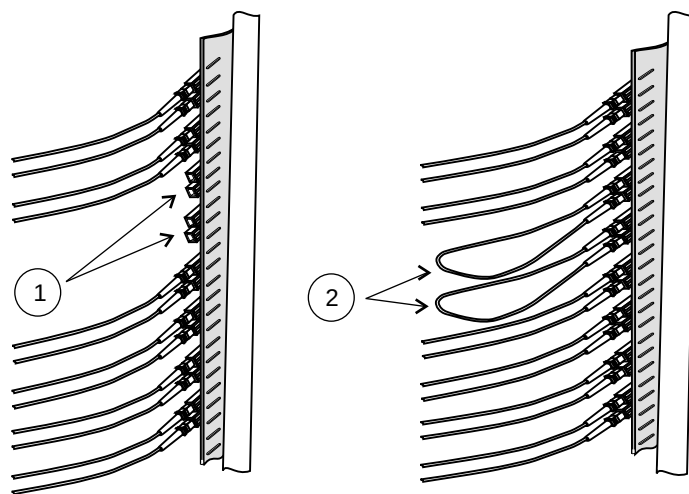
- 1** To save yourself time and possible service interruption, read “Background information” (12-2).
- 2** Query the unit at *Provision > Equipment > Unit*. Verify that the unit you are testing displays `Unit provisioned and initialised` in the Unit Status field.
- 3** Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes.

END OF STEPS

Setting up looparound cables

Important! There is no need to add looparound cables to ports that are already connected to subracks.

-
- 1 If there are spare ports on the BSSU, obtain one SC/SC optical cable for every *spare* port.
-
- 2 Connect one end of the SC/SC optical cable to the transmit side of the port, and the other end to the receive side.



Legend:

1. Spare ports
2. Looparound cables

-
- 3 If there are other spare ports, install cables for those ports.

END OF STEPS

Running an Optical Loopback diagnostic test

- 1 Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.

- 2 Select the Unit ID address as MS-3-BSSU-{1–10}.

- 3 Select External in the Test Type field.

Result:

The system automatically populates the Test field as Optical Loopback and the Loop Count field as 1.

- 4 If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected a number greater than 1 in the Loop Count field.

- 5 Click Execute.

Result:

If you ran the test in the foreground, the system displays the results of the diagnostic test on the screen.

- 6 Remove the looparound cables.

END OF STEPS

Related topics For more information, see one of the following topics:

- If the test failed or errored, see “What to do if the Optical Loopback diagnostic test fails” (12-60).
- For a description of the columns in the Diagnostic Testing - Test Results window, see “Diagnostic Testing - Test Results window” (12-87).
- For a specific description of the Test Results for the Device column, see “Test Results for the Device column description” (12-89).



What to do if the Optical Loopback diagnostic test fails

Procedure

- 1** Verify that the SC/SC optical cables are connected to the correct positions on the BSSU unit.

- 2** Repeat the diagnostic test.

- 3** If the diagnostic test failed, install new SC/SC optical cables.

- 4** Repeat the diagnostic test.

- 5** If the diagnostic test failed, replace the BSSU using the procedure in “Clearing a FLTcEQ on a BSIU or BSSU” (21-57).

- 6** Repeat the diagnostic test.

- 7** If the diagnostic test failed, record the time and date this occurred, and call technical support.

END OF STEPS



STU Station Clock diagnostic test

Overview

Purpose This section contains information about the STU Station Clock diagnostic test.

Organisation This section is organised as follows:

- “STU Station Clock procedure” (12-62)
- “What to do if the Station Clock diagnostic test fails” (12-66)



STU Station Clock procedure

Purpose The STU Station Clock diagnostic tests the ability of the STU to properly detect and phaselock to the station clock input signals.

Do not test LAH103 STU units Use the Station Clock diagnostic test for LAH102 STU units only. The LAH103 STU-64 unit will not pass this diagnostic test. This test was designed for units that accept 2.048 MHz input signals, and the LAH103 accepts only 64 kHz input signals.

Procedure overview The following list describes the procedures required for a Station Clock diagnostic test:

- “Gathering information” (12-62)
- “Setting up the RF splitter” (12-63)
- “Running a Station Clock diagnostic test” (12-64)
- “What to do if the Station Clock diagnostic test fails” (12-66)

Gathering information Do the following steps before running an STU Station Clock diagnostic test.

- 1** To save yourself time and possible service interruption, read “Background information” (12-2).

- 2** Query the unit at *Provision > Equipment > Unit*. Verify that the unit you are testing displays Unit provisioned and initialised in the Unit Status field.

- 3** Query the input timing reference for the station clock at *Provision > Synchronisation and Timing > Station Clock*. Verify that there are no station clock inputs provisioned.

- 4** If there are station clock inputs provisioned, remove them using the Station Clock window.

To remove provisioned station clock inputs, enter the Port ID, select the None field, and click Apply.

- 5** Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes.

END OF STEPS

Setting up the RF splitter

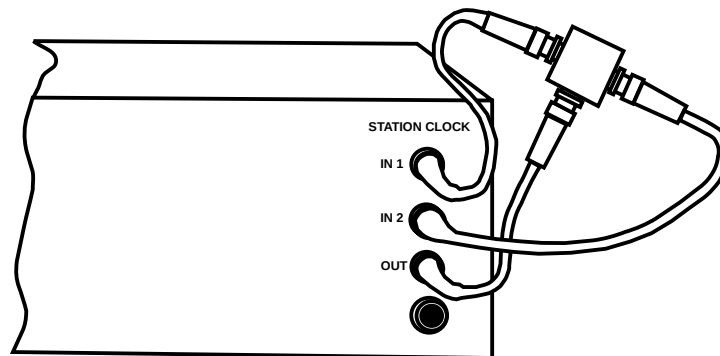
- 1 Obtain one Radio Frequency (RF) splitter (ZFSC-2-1-75-6).
.....
- 2 Locate the Station Clock connectors on the back of the Matrix and Synchronisation subrack.

Reference:

The top subrack panel containing STU-1 should be designated as working, and the bottom panel containing STU-2 should be designated as protection. Choose the appropriate panel for the test you want to run.

.....

- 3 Install the splitter as follows:
 - S (source) to OUT
 - 1 to IN 1
 - 2 to IN 2



END OF STEPS

Running a Station Clock diagnostic test

- 1 Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.

- 2 Select the Unit ID address as MS-3-STU-{1, 2}.

- 3 Select External in the Test Type field.

Result:

The system automatically populates the Test field as Station Clock and the Loop Count field as 1.

- 4 If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected a number greater than 1 in the Loop Count field.

- 5 Click Execute.

Result:

Since the test is potentially service affecting, the system asks you to confirm the command.

- 6 Click yes.

Result:

If you ran the test in the foreground, the system displays the results of the diagnostic test on the screen.

- 7 Remove the splitter from the panel.

END OF STEPS

Related topic If the diagnostic test failed, see “What to do if the Station Clock diagnostic test fails” (12-66).



What to do if the Station Clock diagnostic test fails

Procedure

- 1

Verify that the RF splitter is connected to the correct station clock connectors on the back of the Matrix and Synchronisation subrack. The cable connections should go from station clock panel OUT to the splitter, from the splitter to station clock panel IN 1, and from the splitter to station clock panel IN 2.
- 2

Repeat the diagnostic test.
- 3

If the diagnostic test failed, connect the STU Station Clock IN 1 and OUT with a cable.
- 4

Repeat the diagnostic test.
- 5

If the only failure is on Station Clock IN 2, replace the RF splitter.
- 6

Repeat the diagnostic test.
- 7

If the diagnostic test failed, replace the STU.

Reference:

Use the procedure in “Clearing a FLTcEQ on a BSC or STU” (21-53).
- 8

Repeat the diagnostic test.
- 9

If the diagnostic test failed, record the time and date this occurred, and call technical support.
- END OF STEPS



BSC, BSIU, BSSU, DTU, and STU Unit diagnostic tests

Overview

Purpose This section contains information about the BSC, BSIU, BSSU, DTU, and STU Unit diagnostic tests.

Organisation This section is organised as follows:

- [“BSC Unit procedure” \(12-68\)](#)
- [“BSIU and BSSU Unit procedure” \(12-71\)](#)
- [“DTU Unit procedure” \(12-74\)](#)
- [“STU Unit procedure” \(12-77\)](#)
- [“What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails” \(12-84\)](#)



BSC Unit procedure

Purpose The BSC Unit diagnostic tests the internal hardware on the BSC.

Procedure overview The following list describes the procedures required for a BSC Unit diagnostic test:

- “Gathering information” (12-68)
- “Force the protection state” (12-69)
- “Running a BSC Unit diagnostic test” (12-69)
- “What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails” (12-84)
- “Removing the forced switch” (12-70)

Gathering information Do the following steps before running a BSC Unit diagnostic test.

- 1** To save yourself time and possible service interruption, read “Background information” (12-2).
- 2** Query the unit at *Provision > Equipment > Unit*. Verify that the unit you are testing displays Unit provisioned and initialised in the Unit Status field.
- 3** Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes.

END OF STEPS

Force the protection state Perform the following steps to make sure that the BSC unit you are testing is in the standby state.

- 1 Query the protection status of the Matrix and Synchronisation subrack.

Reference:

Use the MS Control window at *Protection > Equipment > MS Control*.

- 2 If necessary, perform a Force Switch to Working or Force Switch to Protect to make the subrack standby.

Reference:

Use the MS Control window at *Protection > Equipment > MS Control*.

END OF STEPS

**Running a BSC Unit
diagnostic test**

Important! You can perform BSC Unit tests only on BSC units that are located on the standby Matrix and Synchronisation subrack.

- 1 Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.

- 2 Select the standby BSC unit in the Unit ID field.

Result:

The system automatically populates the Test Type field as Internal, the Test field as Unit, and the Loop Count field as 1.

- 3 If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected a number greater than 1 in the Loop Count field.

- 4 Click Execute.

Result:

If the unit is in the correct protection state, the window displays a list of units whose service may be affected by the diagnostic test.

-
- 5** Click yes if you want to continue.

END OF STEPS

Related topic

If the diagnostic test fails, see “What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails” (12-84).

Removing the forced switch

Do the following steps if you had to perform a Force Switch to Working or Force Switch to Protect to make the subrack standby. The purpose of doing this is not to switch service back to the original state, but to remove the forced switch.

-
- 1** Go to the MS Control window at *Protection > Equipment > MS Control*.

-
- 2** Click Clear Forced Switch.

-
- 3** Click Apply.

END OF STEPS



BSIU and BSSU Unit procedure

Purpose BSIU and BSSU Unit diagnostics test the internal hardware on the BSIU or BSSU.

Procedure overview The following list describes the procedures required for a BSSU Unit or a BSIU Unit diagnostic test:

- “Gathering information” (12-71)
- “Force or lock the protection state” (12-72)
- “Running a BSIU or BSSU Unit diagnostic test” (12-72)
- “What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails” (12-84)
- “Clear the protection state” (12-73)

Gathering information Do the following steps before running a BSIU or BSSU Unit diagnostic test.

- 1** To save yourself time and possible service interruption, read “Background information” (12-2).
- 2** Query the unit at *Provision > Equipment > Unit*. Verify that the unit you are testing displays Unit provisioned and initialised in the Unit Status field.
- 3** Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes.

END OF STEPS

Force or lock the protection state

You must force to protection or lock off protection to keep the system from switching to the unit during testing.

- 1 Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.
- 2 Is the unit you want to test the working unit or the protection unit?

If the unit you want to test is	Then
Working (units 1–8)	Force Switch to Protect
Protection (units 9 or 10)	Lock Service Off of Protect

- 3 Click Apply.

END OF STEPS

Running a BSIU or BSSU Unit diagnostic test

- 1 Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.
- 2 Select the BSSU or BSIU Unit ID address.
- 3 Select Internal in the Test Type field.

Result:

The system automatically populates the Test field as Unit, and the Loop Count field as 1.

- 4 If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected a number greater than 1 in the Loop Count field.

- 5 Click Execute.

Result:

If the protection state is set to Force Switch to Protect or Lock Service Off of Protect, the window displays a list of units whose service may be affected by the diagnostic test.

-
- 6** Click yes if you want to continue.

END OF STEPS

Related topic

If the diagnostic test fails, see “What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails” (12-84).

Clear the protection state

-
- 1** Go to the Matrix Slice window at *Protection > Equipment > Matrix Slice*.

-
- 2** Click Clear Forced Switch or Clear Lock Off.

-
- 3** Click Apply.

END OF STEPS



DTU Unit procedure

Purpose The DTU unit diagnostic tests the internal hardware on the DTU.

Procedure overview The following list describes the procedures required for a DTU Unit diagnostic test:

- “Gathering information” (12-74)
- “Force the protection state” (12-75)
- “Running a DTU Unit diagnostic test” (12-75)
- “What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails” (12-84)
- “Removing the forced switch” (12-76)

Gathering information Do the following steps before running a DTU Unit diagnostic test.

- 1** To save yourself time and possible service interruption, read “Background information” (12-2).
- 2** Query the unit at *Provision > Equipment > Unit*. Verify that the unit you are testing displays Unit provisioned and initialised in the Unit Status field.
- 3** Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes.

END OF STEPS

Force the protection state Perform the following steps to make sure that the DTU unit you are testing is in the standby state.

- 1 Query the protection status of the DTU unit.

Reference:

Use the DTU window at *Protection > Equipment > DTU*.

- 2 If necessary, perform a Force Switch to Working or Force Switch to Protect to make the subrack standby.

Reference:

Use the DTU window at *Protection > Equipment > DTU*.

END OF STEPS

**Running a DTU Unit
diagnostic test**

- 1 Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.

- 2 Select the standby DTU unit in the Unit ID field.

Result:

The system automatically populates the Test Type field as Internal, the Test field as Unit, and the Loop Count field as 1.

- 3 If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected a number greater than 1 in the Loop Count field.

- 4 Click Execute.

Result:

If the unit is in the correct protection state, the window displays a list of units whose service may be affected by the diagnostic test.

- 5 Click yes if you want to continue.

END OF STEPS

Related topic

If the diagnostic test fails, see “What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails” (12-84).

Removing the forced switch

Do the following steps if you had to perform a Force Switch to Working or Force Switch to Protect to make the unit standby. The purpose of doing this is not to switch service back to the original state, but to remove the forced switch.

- 1 Go to the DTU window at *Protection > Equipment > DTU*.
- 2 Click Clear Forced Switch.
- 3 Click Apply.

END OF STEPS



STU Unit procedure

Purpose	The STU unit diagnostic tests the internal hardware on the STU.
Procedure overview	The following list describes the procedures required for an STU Unit diagnostic test: • “Gathering information” (12-77) • “Force the protection state” (12-78) • “Running an STU Unit diagnostic test” (12-78) • “What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails” (12-84) • “Removing the forced switch” (12-79)
Gathering information	Do the following steps before running an STU Unit diagnostic test. 1 To save yourself time and possible service interruption, read “Background information” (12-2). 2 Query the unit at <i>Provision > Equipment > Unit</i>. Verify that the unit you are testing displays <code>Unit provisioned</code> and <code>initialised</code> in the Unit Status field. 3 Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes. END OF STEPS

Force the protection state Perform the following steps to make sure that the STU unit you are testing is in the standby state.

- 1 Query the protection status of the Matrix and Synchronisation subrack.

Reference:

Use the MS Control window at *Protection > Equipment > MS Control*.

- 2 If necessary, perform a Force Switch to Working or Force Switch to Protect to make the subrack standby.

Reference:

Use the MS Control window at *Protection > Equipment > MS Control*.

END OF STEPS

**Running an STU Unit
diagnostic test**

- 1 Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.

- 2 Select the standby STU unit in the Unit ID field.

- 3 Select the Test Type as Internal.

Result:

The system automatically populates the Test field as Unit, and the Loop Count field as 1.

- 4 If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected a number greater than 1 in the Loop Count field.

- 5 Click Execute.

Result:

If the subrack is in the correct protection state, the window displays a list of units whose service may be affected by the diagnostic test.

-
- 6** Click yes if you want to continue.

END OF STEPS

Related topic

If the diagnostic test fails, see “What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails” (12-84).

Removing the forced switch

Do the following steps if you had to perform a Force Switch to Working or Force Switch to Protect to make the subrack standby. The purpose of doing this is not to switch service back to the original state, but to remove the forced switch.

-
- 1** Go to the MS Control window at *Protection > Equipment > MS Control*.
-
- 2** Click Clear Forced Switch.
-
- 3** Click Apply.

END OF STEPS



All other equipment diagnostic tests

Overview

Purpose This section contains information about equipment diagnostic tests for most test types.

Organisation This section is organised as follows:

- [“All other equipment diagnostic tests” \(12-81\)](#)
- [“What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails” \(12-84\)](#)
- [“What to do if the Network Interface test fails” \(12-85\)](#)
- [“What to do if the MD Inputs diagnostic test fails” \(12-54\)](#)
- [“What to do if the MCLAN diagnostic test fails” \(12-86\)](#)



All other equipment diagnostic tests

Purpose Use this procedure to run Checksum, Disk Media, IIC, MCLAN, Network Interface, NVRAM, Register Test, Sanity Timer, and port Unit tests.

Procedure overview The following list describes the procedures required for Checksum, Disk Media, IIC, MCLAN, Network Interface, NVRAM, Register Test, Sanity Timer, and port Unit tests:

- “Gathering information” (12-81)
- “Running a diagnostic test” (12-82)
- “What to do if the Network Interface test fails” (12-85)
- “What to do if the MCLAN diagnostic test fails” (12-86)
- “What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails” (12-84)

Gathering information Do the following steps before running a diagnostic test.

- 1** To save yourself time and possible service interruption, read “Background information” (12-2).
- 2** Query the unit at *Provision > Equipment > Unit*. Verify that the unit you are testing displays Unit provisioned and initialised in the Unit Status field.
- 3** Record the number of alarms that appear on the Alarm Panel before you run any diagnostic tests. Diagnostic tests may cause alarms on units indirectly affected by the diagnostic test. These alarms should clear after the diagnostic test completes.

END OF STEPS

Running a diagnostic test

- 1** Go to the Diagnostic Tests window at *Maintenance > Execute Tests > Diagnostic Tests*.
-

- 2** Select the Unit ID.
For port units, if you want to run a test on all the units, select ALL in the last subfield.
-

- 3** Select Internal in the Test Type field if the system has not automatically populated it.
-

- 4** Select the test you want to run in the Test field if the system has not automatically populated it.
-

- 5** If you want the diagnostic test to run more than once, change the Loop Count field to a number greater than 1.

Result:

The Background Test check box is unavailable if you selected ALL in the Unit ID field, or a number greater than 1 in the Loop Count field.

.....

- 6** Click Execute.

Result:

If the test is potentially service affecting, the system asks you to confirm the command.

.....

- 7** Click yes.

END OF STEPS

.....

Related topics

If the diagnostic test fails, see one of the following topics:

- “What to do if the Network Interface test fails” (12-85)
- “What to do if the MCLAN diagnostic test fails” (12-86)
- “What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails” (12-84)



What to do if a Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or Unit diagnostic test fails

Purpose Use this procedure to clear failures for Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, and Unit tests.

Procedure

1 Run the test again.

.....

2 If the test failed again, replace the unit.

Reference:

For the appropriate unit-replacement procedure, see “FLTcEQ flowcharts and procedures” (21-48).

.....

3 Repeat the test.

.....

4 Did the test pass or fail?

If the test	Then
Passed	Return the defective unit to technical support.
Failed again	Record the time and date this occurred, and call technical support.

END OF STEPS

.....



What to do if the Network Interface test fails

Procedure

- 1 Verify that the cable connectors of the MPU NIC port that failed are connected to the correct port locations.

Reference:

For information about which port failed the test, see “Failure codes” (12-103).

- 2 Repeat the test.
-

- 3 If the test fails again, install a new MPU MC port-to-hub cable.
-

- 4 Repeat the diagnostic test.
-

- 5 If the diagnostic test fails again, replace the MPU.

Reference:

For the unit replacement procedure, see “Clearing a FLTcEQ on an MPU” (21-69).

- 6 Repeat the diagnostic test.
-

- 7 If the diagnostic test fails again, record the time and date this occurred, and call technical support.

END OF STEPS



What to do if the MCLAN diagnostic test fails

Procedure

- 1 Verify that the cable connectors of the LHU MCLAN port that failed are connected to the correct port locations.

Reference:

For information about which port failed the diagnostic test, see “Failure codes” (12-103).

- 2 Repeat the diagnostic test.

- 3 If the diagnostic test fails again, install a new LHU MCLAN cable.

- 4 Repeat the diagnostic test.

- 5 If the diagnostic test fails again, replace the LHU.

Reference:

For the unit replacement procedure, see “Clearing a FLTcEQ on an ARU, LHU, or PSP” (21-51).

- 6 Repeat the diagnostic test.

- 7 If the diagnostic test fails again, record the time and date this occurred, and call technical support.

END OF STEPS



Diagnostic Testing - Test Results window

Overview

Purpose This section describes the diagnostic test results that display after a diagnostic test is run.

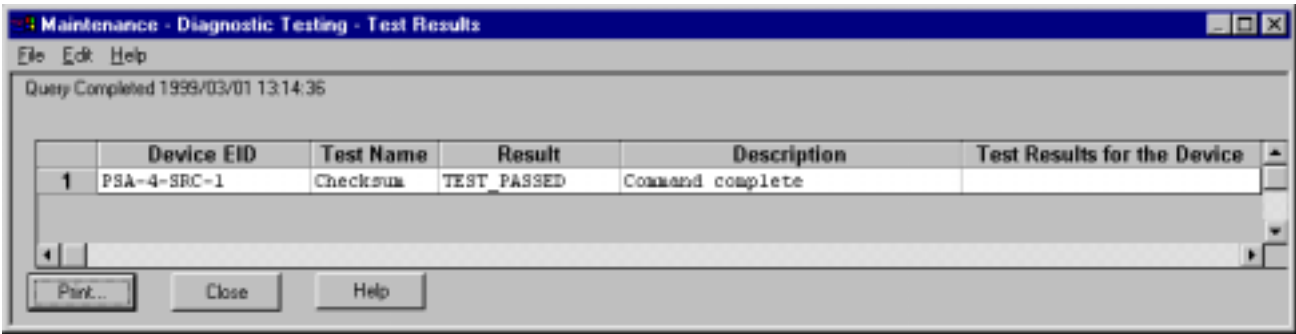
Organisation This section is organised as follows:

- “Diagnostic Testing - Test Results window description” (12-88)
- “Test Results for the Device column description” (12-89)



Diagnostics Testing - Test Results window description

Illustration The following illustration shows an example of a Diagnostic Testing - Test Results window that displays when you run a diagnostic test from the Diagnostic Tests window.



Results field descriptions The following information appears in the Diagnostic Testing - Test Results window.

Column	Description
Device EID	Specifies the entity address of the equipment that the system tested.
Test Name	The name of the test (Optical Loopback, Checksum, BCLAN...) that you ran.
Result	Displays the result of the test as one of the following: • TEST_PASSED • PARTIAL_PASSED • TEST_FAILED • TEST_ERRORED
Description	If the test errors, this column lists the return code and a brief description. If the test fails, this column will provide a brief description of the failure.
Test Results for the Device	If the diagnostic test fails or errors, this column provides specific information about what caused the failure or error. For more information, see “Test Results for the Device column description” (12-89).

Related topic For general information about windows, see “About the main application window” (4-10).



Test Results for the Device column description

**BCLAN, SONIC, MCLAN,
and DFWT STM-1 electrical
diagnostic tests**

When a diagnostic test fails or errors, the Test Results for the Device column (also called the 64-byte field) gets populated with values. For a failure of a BCLAN, SONIC, MCLAN, and DFWT STM-1 electrical diagnostic test, use these values to determine which unit or port failed.

All other diagnostic tests

For all other tests, these byte values can provide more specific information — but keep in mind that for all tests except the BCLAN, SONIC, MCLAN, or DFWT STM-1 electrical, these byte values were designed to be used by factory personnel, and may not be useful to most users. The important thing to know is that the unit failed the diagnostic test, and that it may need to be replaced.

Related topics

For more information about the values in the 64-byte field see one of the following topics:

- “How to interpret BCLAN failure results” (12-23)
- “How to interpret which electrical STM-1 IU failed” (12-48)
- “Byte descriptions for equipment diagnostic tests” (12-91)
- “Test codes” (12-93)
- “Failure codes” (12-103)
- “Error codes” (12-106)



Diagnostic Testing - Test Results

Overview

Purpose This section is used by factory personnel to determine the meaning of the byte values in the Test Results for the Device column of the Diagnostic Testing - Test Results window.

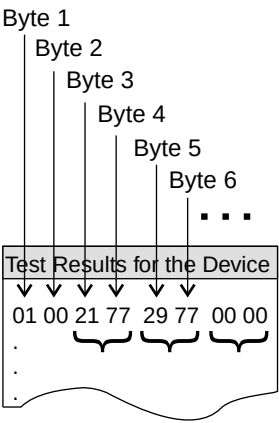
Organisation This section is organised as follows:

- “Byte descriptions for equipment diagnostic tests” (12-91)
- “Test codes” (12-93)
- “Failure codes” (12-103)
- “Error codes” (12-106)



Byte descriptions for equipment diagnostic tests

Byte positions The following graphic describes the positions of the bytes.



Paired bytes The pairs that are grouped within the braces in the diagram are interpreted together. The number of byte pairs populated with information depends on how many tests failed or errored the diagnostic test.

Pairs of codes are displayed in subsequent bytes if more tests failed or errored.

Byte meanings The bytes in the Test Results for the Device column contain the following information.

Byte	Description
1	The following describes the meaning of byte 1: • 00 = passed • 01 = failed • 02 = errored • 03 = partial passed
2	Byte 2 is applicable only for a DFWT STM-1 electrical test or button test. See “How to interpret which electrical STM-1 IU failed” (12-48).
3	Byte 3 displays a <i>test number</i> for the first test that failed or errored. To interpret the codes, see the Test code tables.

Byte	Description
4	Bytes 3 and 4 are interpreted together. Byte 4 describes the <i>reason</i> why the test described in byte 3 failed or errored. For a description of the codes that may appear in byte 4, see the Failure code table or the Error code table.
5	Byte 5 displays a test number for the second test that failed or errored, if a second test failed or errored.
6	Bytes 5 and 6 are interpreted together. Byte 6 describes the <i>reason</i> why the test described in byte 5 failed or errored.

Pairs of codes are displayed in subsequent bytes if more tests failed or errored.



Test codes

BSC The following list describes the meanings of the BSC test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	Initialise Picard
02	Picard Control Register Access
03	OLU 1 is present in IIC test
04	OLU 2 is present in IIC test
05	FPGA Register Access
06	Interrupt
07	BSFI RAM
08	Communication Channel Loopback
09	PCI Loopback
0a	BSFI Framer Loopback

BSIU The following list describes the meanings of the BSIU test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
13	PCI
14	EPI 1
15	EPI 2
16	EPI 3
17	EPI 4
18	EPI 5
19	EPI 6
1a	EPI 7
1b	EPI 8
1c	EPI 9
1d	EPI 11
1e	EPI 12

Value in bytes 3, 5, 7...	Description
1f	EPI 13
20	EPI 14
21	EPI 15
22	EPI 16
23	EPI 17
24	EPI 18
25	EPI 19
26	ECI 1
27	ECI 2
28	ECI 3
29	ECI 4
2A	Inventory
2B	BIST

BSSU The following list describes the meanings of the BSSU test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	BSSU board logic
02	BSSU BSFI
11	BSSU Tsunami #1
12	BSSU Tsunami #2
13	BSSU Tsunami #3
14	BSSU Tsunami #4
15	BSSU Tsunami #5
16	BSSU Tsunami #6
17	BSSU Tsunami #7
18	BSSU Tsunami #8
19	BSSU Tsunami #9
1a	BSSU Tsunami #10
1b	BSSU Tsunami #11

Value in bytes 3, 5, 7...	Description
1c	BSSU Tsunami #12
1d	BSSU Tsunami #13
1e	BSSU Tsunami #14
1f	BSSU Tsunami #15
20	BSSU Tsunami #16
21	BSSU Taifu #1
22	BSSU Taifu #2
23	BSSU Taifu #3
24	BSSU Taifu #4
25	BSSU Taifu #5
26	BSSU Taifu #6
27	BSSU Taifu #7
28	BSSU Taifu #8
31	ASIC 1/2 ring test
32	ASIC 2/3 ring test
33	ASIC 3/4 ring test
34	ASIC 4/5 ring test
35	ASIC 5/6 ring test
36	ASIC 6/7 ring test
37	ASIC 7/8 ring test
38	ASIC 8/1 ring test

BSSU Optical Loopback

The following list describes the meanings of the BSSU Optical Loopback test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
41	BSSU Optical Loop 1
42	BSSU Optical Loop 2
43	BSSU Optical Loop 3
44	BSSU Optical Loop 4
45	BSSU Optical Loop 5

Value in bytes 3, 5, 7...	Description
46	BSSU Optical Loop 6
47	BSSU Optical Loop 7
48	BSSU Optical Loop 8
49	BSSU Optical Loop 9
4a	BSSU Optical Loop 10
4b	BSSU Optical Loop 11
4c	BSSU Optical Loop 12
4d	BSSU Optical Loop 13
4e	BSSU Optical Loop 14
4f	BSSU Optical Loop 15
50	BSSU Optical Loop 16

Checksum The following list describes the meanings of the Checksum test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	EAPROM Checksum

Disk Media The following list describes the meanings of the Disk Media test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	First read/write

DTU The following list describes the meanings of the DTU test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	Picard Dual Port RAM
02	Picard FPGA Program

Value in bytes 3, 5, 7...	Description
03	Picard Control Register
04	Picard BCLAN Address
05	Picard BCLAN Loopback
06	DTU Picard Control Register
07	Picard Status Register
08	Picard STOH Register Test
09	Picard FPGA
0a	PCI Receive Register
0b	PCI Receive RAM
0c	PCI Transmit Register
0d	PCI Transmit RAM
0e	DPLL Shared RAM
0f	PCL Loopback
10	DPLL Download
11	DPLL Boot
12	DPLL Diagnostic

IIC The following list describes the meanings of the IIC test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	IIC read/write
02	IIC checksum

MCLAN Cable The following list describes the meanings of the MCLAN Cable test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	MCLAN Port 1
02	MCLAN Port 2
03	MCLAN Port 3

Value in bytes 3, 5, 7...	Description
04	MCLAN Port 4
05	MCLAN Port 5
06	MCLAN Port 6
07	MCLAN Port 7
08	MCLAN Port 8
09	MCLAN Port 9
0a	MCLAN Port 10
0b	MCLAN Port 11
0c	MCLAN Port 12
0d	MCLAN Port 13
0e	MCLAN Port 14
0f	MCLAN Port 15
10	MCLAN Port 16
11	MCLAN Port 17
12	MCLAN Port 18

MD Inputs The following list describes the meanings of the MD Inputs test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	MD Alarm Input 1
02	MD Alarm Input 2
03	MD Alarm Input 3
04	MD Alarm Input 4

Network Interface The following list describes the meanings of the Network Interface test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	Graphical User Interface (GUI) to working MC
03	GUI to SRC

NVRAM The following list describes the meanings of the NVRAM test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	MPU NVRAM

Register Test The following list describes the meanings of the Register Test test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	Control Register

Sanity Timer (ARU) The following list describes the meanings of the Sanity Timer (ARU) test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	ARU Watchdog Timer
02	MPU Sanity Timer

Sanity Timer (SRC) The following list describes the meanings of the Sanity Timer (SRC) test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	Sanity Timer

STM-1, STM-4, and STM-16 The following list describes the meanings of the port unit test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	SPECTRA 1 device
02	SPECTRA 2 device

Value in bytes 3, 5, 7...	Description
03	SPECTRA 3 device
04	SPECTRA 4 device
05	SPECTRA 5 device
06	SPECTRA 6 device
07	SPECTRA 7 device
08	SPECTRA 8 device
09	SPECTRA 9 device
0a	SPECTRA 10 device
0b	SPECTRA 11 device
0c	SPECTRA 12 device
0d	Port 1 Loopback device
0e	Port 2 Loopback device
0f	Port 3 Loopback device
10	Port 4 Loopback device
11	Port 5 Loopback device
12	Port 6 Loopback device
13	Port 7 Loopback device
14	Port 8 Loopback device
15	Port 9 Loopback device
16	Port 10 Loopback device
17	Port 11 Loopback device
18	Port 12 Loopback device
19	TUPP 1 device
1a	TUPP 2 device
1b	TUPP 3 device
1c	TUPP 4 device
1d	TRANSPORTER ASIC device
1e	STM-0 Initialise Picard
1f	STM-1 Initialise Picard
20	Interface Unit
21	DFWT on port 1
22	DFWT on port 2

Value in bytes 3, 5, 7...	Description
23	DFWT on port 3
24	DFWT on port 4
25	DFWT on port 5
26	DFWT on port 6
27	DFWT on port 7
28	DFWT on port 8
29	DFWT on port 9
2a	DFWT on port 10
2b	DFWT on port 11
2c	DFWT on port 12
2d	STM-4 initialise Picard
2c	STM-16 initialise Picard
2f	CTLID FPGA
30	STS 48 TREP
31	Hermes FPGA

STU The following list describes the meanings of the STU test codes displayed in bytes 3, 5, 7...

Value in bytes 3, 5, 7...	Description
01	Initialise Picard
02	Picard Control Register
03	Picard Status Register
04	BSC Control Register
05	PCI Control Register
06	PCI Downstream MFS Column Row Register
07	PCI Upstream MFS Column Row Register
08	PCI Downstream MFS Frame Register
09	PCI Upstream MFS Frame Register
0a	PCI Loop
0b	DPLL RAM

Value in bytes 3, 5, 7...	Description
0c	DPLL Download
0d	DPLL Boot
0e	DPLL Diagnostics
0f	DPLL Timers Error
10	DPLL 1MS System Interrupt Error
11	DPLL 1MS Cross-Couple Interrupt Error
12	DPLL Unexpected Exception
13	DPLL DCO Error
14	DPLL RAM Test Error
15	DPLL Provisioning Register Error
16	DPLL Status Register Error
17	DPLL Image Checksum Error
18	STU Hardware
19	STU DPLL
1a	STU Station Clock



Failure codes

List of failure codes The following describes the meanings of the failure codes displayed in bytes 4, 6, 8...

Value in bytes 4, 6, 8...	Description
05	I/O error
51	MD Alarm Input Failure
52	File Write Failure
53	File Read Failure
54	File Read/Write Compare Failure
55	Ping fails
56	Test timed out
60	No error
61	Pattern read does not match expected value
62	FPGA failed to program or respond
63	Out of lock (OOL) condition exists on the entity
64	The unit was not present
65	Bad checksum over inventory data
66	Interrupt not received
67	Defects do not match expected value
68	LOS, LOF, LOM, Estore, or RDI detected unexpectedly
69	Pattern inserted was not received through the loopback
6A	RESET or indication failed to assert
6B	BIST test failed or failed to complete
6C	Transmitted J0 does not match expected value
6D	Received J0 does not match expected value
6E	Device ID does not match expected value
6F	Indicated ECI had LOS, indicating no cable is connected
70	Indicated ECI had no LOS but had LOF, indicating a hardware failure
71	Unable to address the device
72	RAPI test failed

Value in bytes 4, 6, 8...	Description
73	Unit clock test failed
74	Line clock test failed
75	Loopback test failed
76	Mode 0 test failed
77	DFWT test failed
78	Picard could not be addressed
79	PRS monitor cannot sync to PRS generator
7a	PRS monitor detects errors
7b	PRS monitor does not detect inserted errors
7c	Parity errors in ADD bus
7d	Parity errors in DROP bus
7e	Parity errors in transporter bus
7f	The Interface Unit is not present
80	Interface Unit inventory data has checksum error
81	Interface Unit is the wrong type
82	Interface Unit external loop failed (electrical or optical)
83	Interface Unit internal loop failed (electrical only)
84	STU station clock reference failed
85	STU station clock output failed
86	STU StaClkTest LTREF1 failed
87	STU StaClkTest LTREF2 failed
88	ARU Timer failed
89	MPU Sanity Timer failed
C1	Faulty cable or connector
C2	One of the following conditions exist: • There is a defective cable from the SRC to the MCLAN hub port • There is a missing connection from the SRC to the MCLAN hub port • The system is unable to communicate with the SRC.
C3	Cabling error (the SRC is connected to the wrong MCLAN hub port)

Value in bytes 4, 6, 8...	Description
D0	Reset or indicator failed to clear
D1	No access to the device
D2	Failed cross-connect test
D3	Ring anomalies detected
D4	BSSU Y2 asserted
FF	Common failure

Error codes

List of error codes The following describes the meanings of the error codes displayed in bytes 4, 6, 8...

Value in bytes 4, 6, 8...	Description
04	Interrupted system call
06	No such device or address
09	Bad file number
0b	No more processes
0e	Bad address (EFAULT)
13	No such device (ENODEV)
16	Invalid argument
1b	File too large
1c	No space left on device
20	Broken pipe
22	Range error in FP library
42	BCLAN drive error
43	Communication failure — tm_send_bcc
44	Database failure
49	Invalid state (working unit must be active)
4c	Trying to read unreadable message
4e	No units were tested
4f	Error creating file
52	The link has been severed
53	Protection switch failure
63	Communication failure — tmt_tm_send to gsync
69	Interface Unit not equipped
6e	No Interface Unit specified
77	Wrong state (maintenance or booting)
83	MTM process restart signal
84	Database read failure
85	System communication services failed
86	MUH completed unsuccessfully

Value in bytes 4, 6, 8...	Description
87	Bad argument in ping call
88	System error during ping call
89	Port is connected to host
8a	Ping call returned unexpected value
8b	File remove failed
8c	MFM command unsuccessful
8d	EID to port conversion failed
8e	Unable to set timer
8f	Checkpointing failed
90	Test not run
93	Unit not in proper state to run this test
94	Test Request field invalid
95	DPLL message send failed for PROV_STAT_CLK_OUT
96	TCP/IP error / DPLL message send failed SYC_REF_1 prov
97	DPLL message send failed for SYC_REF_2 prov
98	DPLL message send failed for RD_STC_OUTPUT_STAT
99	DPLL message send failed for RD_LTREF_STAT
9a	Cross couple between STUs is bad





13 Execute alarm indicator, LED, and button tests

Overview

- Purpose** “Execute alarm indicator, LED, and button tests” contains the following information:
- General information about alarm indicator tests
 - Descriptions of the windows that are used to run diagnostic tests
 - Step-by-step procedures for running diagnostic tests on the alarm indicators, LEDs, and buttons
- Organisation** “Execute alarm indicator, LED, and button tests” is organised as follows:
- “Background information” (13-2)
 - “Alarm Indicator Tests window and procedures” (13-5)
 - “LED Tests window and procedures” (13-16)
 - “Button Tests window and procedures” (13-21)



Background information

Overview

Purpose This section contains background information about alarm indicator and LED diagnostic tests.

Organisation This section is organised as follows:

- “Alarm indicator test terms” (13-3)
- “LEDS on PTMs” (13-4)



Alarm indicator test terms

- List of terms**
- Alarm indicator** An alarm indicator is a visual or audible indication that an alarm is active. One example of an alarm indicator is the red LED on a unit. The red LED lights if a unit fails.
- Deferred test** Tests the Deferred indicator on the User Panel.
- Deferred Maintenance test** Tests the Deferred Maintenance indicator for end-of-suite, rack-top, and station alarms.
- Deferred Maintenance Disconnectable test** Tests the Deferred Maintenance Disconnectable indicator for station alarms.
- Disconnected test** Tests the Disconnected indicator for station alarms and the User Panel.
- Information Alarm test** Tests the Information alarm indicator on the User Panel.
- Output{1–3} test** Tests the miscellaneous discrete output relays 1 through 3.
- Power Failure test** Tests the Power Failure indicator for station alarms and the User Panel.
- Power Failure Disconnectable test** Tests the Power Failure Disconnectable indicator for station alarms.
- Prompt test** Tests the Prompt indicator on the User Panel.
- Prompt Maintenance test** Tests the Prompt Maintenance indicator for end-of-suite, rack-top, and station alarms.
- Prompt Maintenance Disconnectable test** Tests the Prompt Maintenance Disconnectable indicator for station alarms.
- Suppressed test** Tests the Suppressed indicator for station alarms or at the User Panel.



LEDs on PTMs

LEDs on the PTMs during tests

On the Matrix/Synchronisation and port subracks, you will see several Power Terminal Modules (PTMs) that have LEDs on them. The system will not turn on these LEDs during an LED test. However, the LEDs on the BSIU, IU, and BSSU units will light. The LED on a PTM will light only when there is a fuse failure.



Alarm Indicator Tests window and procedures

Overview

Purpose The Alarm Indicator Tests window is used to test the alarm indicators on the Main Controller subrack, the Matrix/Synchronisation subrack, and the port subracks. The alarm indicator test will test the alarm indicators by turning the indicators on and off.

There are two types of alarm interface tests:

- ARU tests on the Main Controller subrack
- SRC tests on the Matrix/Synchronisation and port subracks

Window location *Maintenance > Execute Tests > Alarm Indicator Tests*

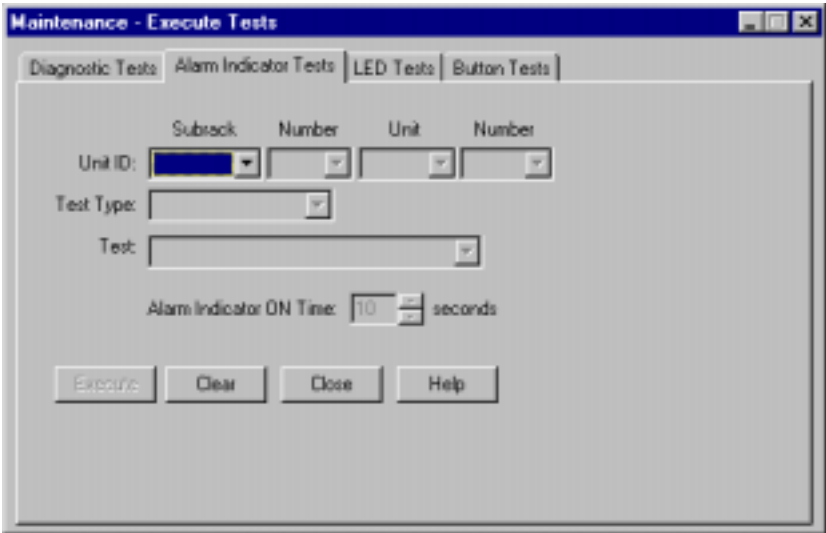
Organisation This section is organised as follows:

- [“Alarm Indicator Tests window description” \(13-6\)](#)
- [“Running an alarm indicator test” \(13-8\)](#)
- [“Proving the standby SRC can turn off an alarm indicator” \(13-10\)](#)
- [“What to do if an MC end-of-suite alarm indicator test fails” \(13-11\)](#)
- [“What to do if an MS or port subrack end-of-suite alarm indicator test fails” \(13-12\)](#)
- [“What to do if an MC rack-top alarm indicator test fails” \(13-13\)](#)
- [“What to do if an MS or port subrack rack-top alarm indicator test fails” \(13-14\)](#)
- [“What to do if a User Panel alarm indicator test fails” \(13-15\)](#)



Alarm Indicator Tests window description

Illustration The following illustration shows the Alarm Indicator Tests window.



Field descriptions The Alarm Indicator Tests window has the following fields.

Field name	Description
Unit ID	The Unit ID field specifies the physical location of the unit you want tested. For a description of the Unit IDs, see “About physical layer addresses” (5-3).
Test Type	The Test Type field specifies the location of the alarm indicators that you want tested as one of the following locations: • “End-of-suite alarm indicators” (6-9) • “MDIs and MDOs” (6-10) • “Rack-top alarm indicators” (6-9) • “Station alarm indicators” (6-9) • “User Panel” (1-20)
Test	The Test field specifies which alarm indicator to test. For a description of each test, see “Alarm indicator test terms” (13-3).
Alarm Indicator ON Time	The Alarm Indicator ON Time field specifies the length of time (1–600 seconds) that the alarm interface test will run. The default value is 10 seconds.

Related topic For general information about windows, see “About the main application window” (4-10).



Running an alarm indicator test

Procedure

- 1 Go to the Alarm Indicator Tests window at *Maintenance > Execute Tests > Alarm Indicator Tests*.

- 2 Select the ARU or SRC address in the Unit ID field.

- 3 Select the location of the alarm indicator in the Test Type field.

Reference: For more information about the options in this field, see one of the following topics:

- “End-of-suite alarm indicators” (6-9)
- “MDIs and MDOs” (6-10)
- “Rack-top alarm indicators” (6-9)
- “Station alarm indicators” (6-9)
- “User Panel” (1-20)

- 4 Select which alarm interface test to run in the Test field.

Reference:

For more information about the options in this field, see “Alarm indicator test terms” (13-3).

- 5 In the Alarm Indicator ON Time field, select how long you want the alarm interface test to run.

- 6 Click Execute.

- 7 Visually check the alarm indicators to make sure that the test was successful. The system will not return any test results.

END OF STEPS

Related topics

For more information, see one of the following topics:

- “Proving the standby SRC can turn off an alarm indicator” (13-10)
- “What to do if an MC end-of-suite alarm indicator test fails” (13-11)
- “What to do if an MS or port subrack end-of-suite alarm indicator test fails” (13-12)
- “What to do if an MC rack-top alarm indicator test fails” (13-13)
- “What to do if an MS or port subrack rack-top alarm indicator test fails” (13-14)
- “What to do if a User Panel alarm indicator test fails” (13-15)



Proving the standby SRC can turn off an alarm indicator

Purpose When running alarm indicator tests on the Matrix and Synchronisation (MS) subrack, if the active SRC in the MS subrack has turned on a rack-top or end-of-suite alarm indicator, the standby SRC in the MS subrack will not be able to turn off the alarm indicator during a test. The following procedure will prove that the standby SRC can turn off an end-of-suite or rack-top alarm indicator.

Procedure Do the following to make sure that the alarm indicator can be turned off. Perform this procedure *after* running an end-of-suite or rack-top alarm test on the active SRC.

1 Suppress the current alarms to extinguish the currently-lit LED.

2 Run the test on the standby SRC.

Result:

This will prove that the LED can be turned on and off from the standby side. Running the test on the active SRC will turn off the alarm indicator, but it will not prove that the standby SRC can control the LED.

END OF STEPS



What to do if an MC end-of-suite alarm indicator test fails

Purpose Use this procedure if you ran a Main Controller end-of-suite alarm indicator test that failed.

Procedure

- 1 Verify that the cable connection from the ACP to the end-of-suite alarm indicator is correct.
.....
- 2 Verify that the cable connection from the ARU to the ACP is correct.
.....
- 3 Run the test again.
.....
- 4 If the test failed again, replace the bulb in the end-of-suite alarm indicator.
.....
- 5 Run the test again.
.....
- 6 Replace the ARU using the procedure in “Clearing a FLTcEQ on an ARU, LHU, or PSP” (21-51).
.....
- 7 Run the test again.
.....
- 8 If the test failed again, call technical support.

END OF STEPS



What to do if an MS or port subrack end-of-suite alarm indicator test fails

Purpose Use this procedure if you ran a Matrix/Synchronisation or port
subrack end-of-suite alarm indicator test that failed.

Procedure

1 Verify that the cable connections from the SRC to the end-of-suite
alarm indicators are correct.

2 Run the test again.

3 If the test failed again, replace the bulb in the end-of-suite alarm
indicator.

4 Run the test again.

5 Replace the SRC.

Reference:

For more information, see “Clearing a FLTcEQ on an SRC”
(21-75).

6 Run the test again.

7 If the test failed again, call technical support.

END OF STEPS



What to do if an MC rack-top alarm indicator test fails

Purpose Use this procedure if you ran a Main Controller rack-top alarm indicator test that failed.

Procedure

1 Verify that the cable connection from the ACP to the rack-top alarm indicator is correct.

2 Verify that the cable connection from the ARU to the ACP is correct.

3 Run the test again.

4 If the test failed again, replace the bulb in the rack-top alarm indicator.

5 Run the test again.

6 Replace the ARU.

Reference:

For more information, see “Clearing a FLTcEQ on an ARU, LHU, or PSP” (21-51).

7 Run the test again.

8 If the test failed again, call technical support.

END OF STEPS



What to do if an MS or port subrack rack-top alarm indicator test fails

Purpose Use this procedure if you ran a Matrix/Synchronisation or port subrack rack-top alarm indicator test that failed.

- Procedure**
- 1

Verify that the cable connections from the SRC to the rack-top alarm indicators are correct.
- 2

Run the test again.
- 3

If the test failed again, replace the bulb in the rack-top alarm indicator.
- 4

Run the test again.
- 5

Replace the SRC.
- Reference:**
For more information, see “Clearing a FLTcEQ on an SRC” (21-75).
- 6

Run the test again.
- 7

If the test failed again, call technical support.
- END OF STEPS



What to do if a User Panel alarm indicator test fails

Procedure

- 1 Verify that the cable connection from the ARU to the ACP is correct.
-

- 2 Verify that the cable connection from the ACP to the User Panel is correct.
-

- 3 Run the test again.
-

- 4 If the test failed again, replace the ARU.

Reference:

For more information, see “Clearing a FLTcEQ on an ARU, LHU, or PSP” (21-51).

- 5 Run the test again.
-

- 6 If the test failed again, replace the failed LED on the User Panel.
-

- 7 Run the test again.
-

- 8 If the test failed again, call technical support.

END OF STEPS



LED Tests window and procedures

Overview

Purpose Use the LED Tests window to light the LEDs on a specific subrack. For the Main Controller subrack, the LEDs on the User Panel will light.

Window location *Maintenance > Execute Tests > LED Tests*

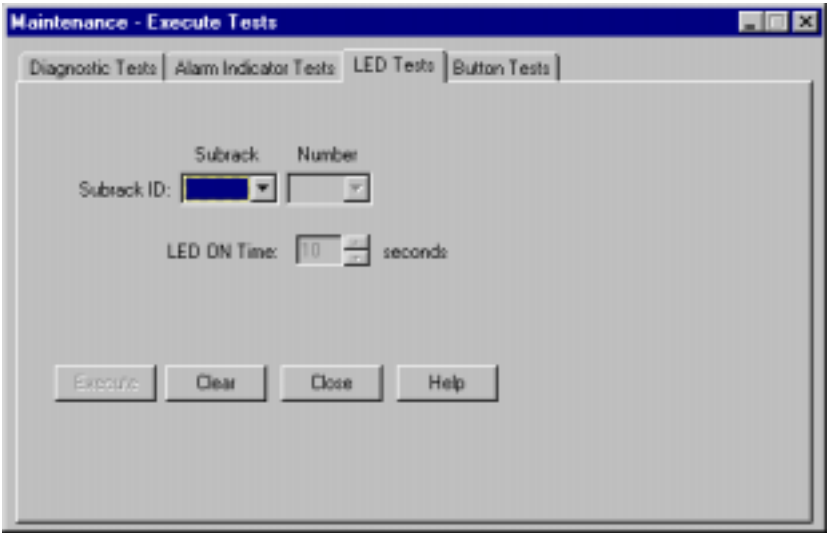
Organisation This section is organised as follows:

- [“LED Tests window description” \(13-17\)](#)
- [“Running an LED test” \(13-18\)](#)
- [“What to do if a unit LED test fails” \(13-19\)](#)
- [“What to do if a User Panel LED test fails” \(13-20\)](#)



LED Tests window description

Illustration The following illustration shows the LED Tests window.



Field descriptions The LED Tests window has the following fields.

Field name	Description
Subrack ID	The Subrack ID field specifies the address of the subrack you want tested.
LED ON Time	The LED ON Time field specifies how long (1–600 seconds, in one-second increments) the LEDs stay lit for the test. The default value is 10 seconds.

Related topic For general information about windows, see “About the main application window” (4-10).



Running an LED test

Procedure

- 1** Go to the LED Tests window at *Maintenance > Execute Tests > LED Tests*.

- 2** Select the Subrack ID.

- 3** Select the LED ON Time.

- 4** Click Execute.

Result:

If you ran an LED test on the Matrix and Synchronisation subrack and only one of the SRCs on the subrack is installed, the test will display LPTP – LED Partial Test Pass. This response means that the system could not test the LEDs on the shelf with the missing SRC.

- 5** Visually check the alarm indicators to make sure that the test was successful. The system will not return any test results.

END OF STEPS

Related topics If the LEDs did *not* light, see one of the following topics:

- “What to do if a unit LED test fails” (13-19)
- “What to do if a User Panel LED test fails” (13-20)



What to do if a unit LED test fails

Procedure Use the following procedure when an LED test on a unit fails:

- 1** Replace the unit.

Reference:

For the appropriate unit-replacement procedure, see “FLTcEQ flowcharts and procedures” (21-48).

- 2** Run the test again.
-

- 3** If the test failed again, call technical support.

END OF STEPS



What to do if a User Panel LED test fails

Procedure Use the following procedure when an LED test on the User Panel fails on the Main Controller (MC) subrack:

1 Verify that the cable connections from the ARU to the User Panel are correct.

2 Run the test again.

3 If the test failed again, replace the ARU.

Reference:

For the ARU unit-replacement procedure, see “Clearing a FLTcEQ on an ARU, LHU, or PSP” (21-51).

4 Run the test again.

5 If the test failed again, replace the failed LED on the User Panel.

6 Run the test again.

7 If the test failed again, call technical support.

END OF STEPS



Button Tests window and procedures

Overview

Purpose Use the Button Tests window to test the following buttons on the User Panel:

- DISCONNECT button
- SUPPRESSED button

The test results for a button test appears in the Result column of the Button Tests - Test Results window.

Window location *Maintenance > Execute Tests > Button Tests*

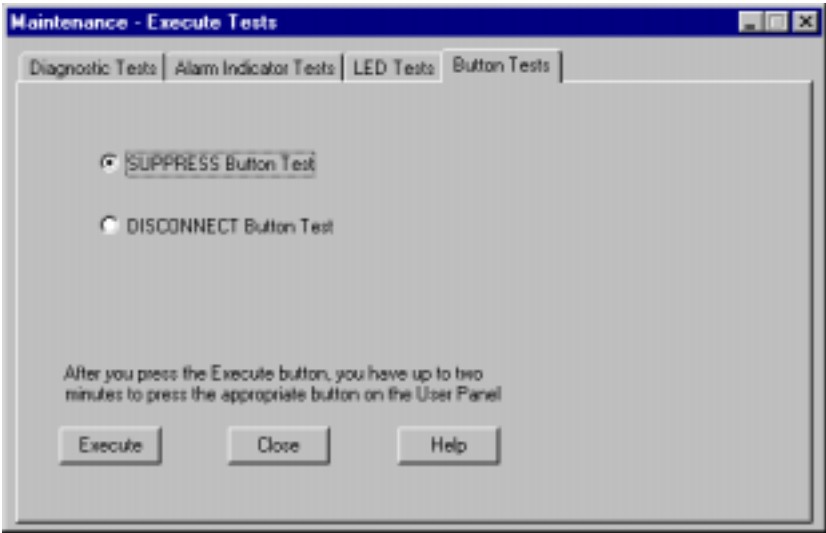
Organisation This section is organised as follows:

- [“Button Tests window description” \(13-22\)](#)
- [“Running a button test” \(13-23\)](#)
- [“Button Testing - Test Results window” \(13-24\)](#)
- [“Byte descriptions for button test” \(13-25\)](#)
- [“What to do if the button test fails” \(13-26\)](#)



Button Tests window description

Illustration The following illustration shows the Button Tests window.



Field descriptions The Button Tests window has the following fields.

Field name	Description
SUPPRESS Button Test	Tests the SUPPRESS button on the User Panel.
DISCONNECT Button Test	Tests the DISCONNECT button on the User Panel.

Related topic For general information about windows, see “About the main application window” (4-10).



Running a button test

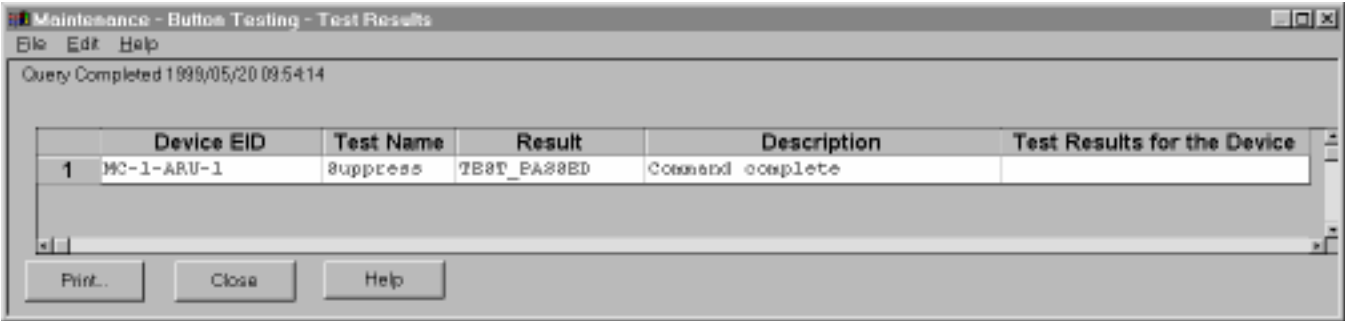
Procedure	
1	Go to the Button Tests window at <i>Maintenance > Execute Tests > Button Tests</i> .
2	Click one of the following tests: - SUPPRESS Button Test - DISCONNECT Button Test
3	Click Execute.
4	Press SUPPRESSED or DISCONNECT on the User Panel.
	END OF STEPS

Related topic If the test fails or errors, see “What to do if the button test fails” (13-26).



Button Testing - Test Results window

Illustration Use the following illustration only as an example of query results from the Button Testing - Test Results window.



Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the Button Testing - Test Results window. Click on a field name to see the field description.

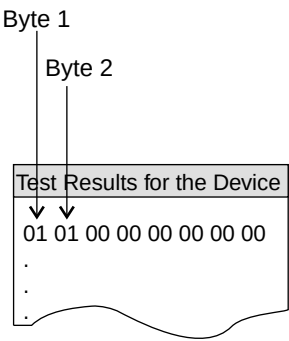
Column	Description
Device ID	Displays the entity address of the equipment that the system tested.
Test Name	Displays the name of the test that you ran.
Result	Displays the result of the test as one of the following: • TEST_PASSED • PARTIAL_PASSED • TEST_FAILED • TEST_ERRORED
Description	If the test errors, this column lists the return code and a brief description. If the test fails, this column will provide a brief description of the failure.
Test Results for the Device	If the test fails or errors, this column provides specific information about what caused the failure or error. For more information, see “Byte descriptions for equipment diagnostic tests” (12-91).

Related topic For general information about windows, see “About the main application window” (4-10).



Byte descriptions for button test

Positions of bytes The following graphic describes the positions of the bytes.



Meaning of bytes The bytes in the Test Results for the Device column contain the following information.

Byte	Description
1	The following describes the meaning of byte 1: • 00 = passed • 01 = failed • 02 = errored
2	The following describes the meaning of byte 2: • 01 = Main Controller (MC)-1 • 02 = MC-2



What to do if the button test fails

Procedure

- 1 Verify that the cable connections from the ACP to the User Panel and from the ARU to the ACP are correct.
-

- 2 Run the test again.
-

- 3 If the test failed again, replace the ARU, and run the test again.

Reference:

For more information, see “Clearing a FLTcEQ on an ARU, LHU, or PSP” (21-51).

- 4 If the test failed again, replace the button on the User Panel.
-

- 5 Run the test again.
-

- 6 If the test failed again, call technical support.

END OF STEPS





14 View test results

Overview

Purpose “View test results” describes how to use the View Test Results window. Use the View Test Results window to query equipment tests that have *completed*.

- To view the test results of a failed test, run the test again in the foreground on the Diagnostic Tests window.
- To view background tests that are still in progress, use the Background Tests window.

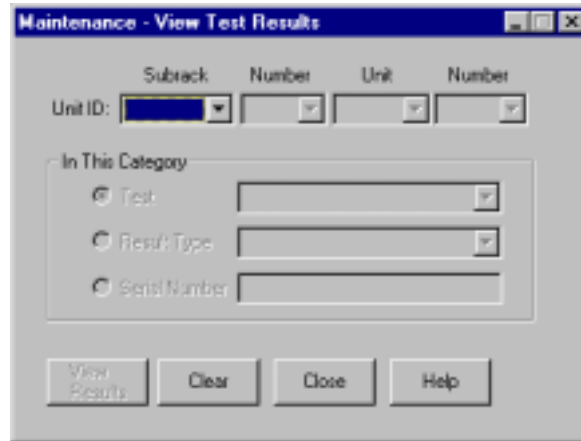
Window location *Maintenance > View Test Results*

Organisation “View test results” is organised as follows:
“View Test Results window description” (14-2)
“How to view completed test results” (14-3)



View Test Results window description

Illustration The following illustration shows the View Test Results window.



Field descriptions The following fields appear on the View Test Results window.

Field name	Description
Unit ID	The Unit ID field specifies the physical location of the unit (circuit pack) that was tested. For a description of the Unit IDs, see “About physical layer addresses” (5-3).
Test	The Test field specifies the diagnostic test that was run. For a list of tests and descriptions, see “Test descriptions” (12-3).
Result Type	You must specify a value in the Result Type field if multiple tests or a loop count was run in the background. Enter the test results you want to view as one of the following: • TEST_PASSED • TEST_FAILED • TEST_ERRORED • TEST_PTP (partial passed) For a definition of these terms, see “Equipment diagnostic test terms” (12-6).
Serial Number	The serial number of the unit that was tested.

Related topic For general information about windows, see “About the main application window” (4-10).



How to view completed test results

Procedure

1

Go to the View Test Results window at *Maintenance > View Test Results*.

2

Select the Unit ID.
Use the ALL wildcard for less-specific address queries.

3

If you want, select values in the Test, Result Type, or Serial Number fields.
You must select at least one of these fields.

4

Click View Results.

END OF STEPS

View Results query

Illustration Use the following illustration only as an example of query results from the View Results window.

	Entity ID	Serial Number	Test Executed	Passed	Partial Pass	Failed	Errored	Date of Execution	Time of Execution
1	PSA-4			73	0	0	27		
2	PSA-5			59	0	0	33		
3	PSA-7			25	0	0	0		

Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the View Results Query window.

Column	Description
Entity ID	The Entity ID column displays the physical address of the port.
Serial Number	The Serial Number column displays the serial number of the unit that was tested.
Test Executed	The Test Executed column displays the diagnostic test that was run.
Passed	The Passed column displays the number of times that the test passed.
Partial Pass	The Partial Pass column displays the number of times that the test partial passed.
Failed	The Failed column displays the number of times that the test failed.
Errored	The Errored column displays the number of times that the test errored.
Date of Execution	The Date of Execution column displays the date that the diagnostic test was run.
Time of Execution	The Time of Execution column displays the time that the diagnostic test was run.

Related topic For general information about windows, see “About the main application window” (4-10).





15 Background tests

Overview

Purpose “Background tests” describes how to use the Background Tests window.

Window location *Maintenance > Background Tests*

Organisation “Background tests” is organised as follows:
“Where to view background tests” (15-2)
“Background Tests window description” (15-3)
“Displaying background tests in progress” (15-4)
“Cancelling a background test” (15-5)



Where to view background tests

Tests in progress Use the Background Tests window to display or cancel one or more background tests that are *in progress*.

Completed tests View the results of *completed* background tests from the View Test Results window.

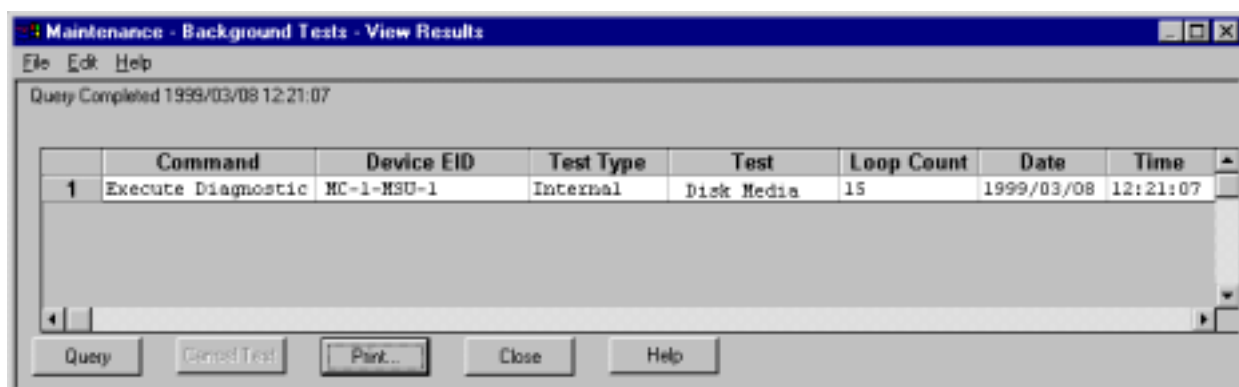
Tip

The results of a foreground test are automatically displayed on the Diagnostic Tests window after the test completes.



Background Tests window description

Illustration The following illustration shows the Background Tests - View Results window.



Field descriptions The Background Tests - View Results window has the following fields.

Field name	Description
Command	The Command field displays the command that was previously entered (for example: Execute Diagnostic).
Device EID	The Device EID field displays the entity address of the unit that was tested.
Test Type	The Test Type field displays the type of diagnostic test as one of the following: - Internal — tests that do not require external cable connections - External — tests that require external cable connections - All — both internal and external tests
Test	The Test field displays the diagnostic test that was requested. For a list of tests and descriptions, see “Test descriptions” (12-3).
Loop Count	The Loop Count field displays the number of times (1–25) that the system repeats the test.
Date	The Date field displays the date of the test.
Time	The Time field displays the time of the test.

Related topic For general information about windows, see “About the main application window” (4-10).



Displaying background tests in progress

Procedure The Alarm Panel displays the number of background tests that are running.

- 1 Go to the Background Tests window at *Maintenance > Background Tests*.

Result:

The Background Tests - View Results window appears on the screen.

END OF STEPS



Cancelling a background test

Procedure

- 1 Go to the Background Tests window at *Maintenance > Background Tests*.

Result:

The Background Tests - View Results window appears on the screen.

- 2 Highlight the test you want to cancel by double-clicking on the row.
-

- 3 Click Cancel Test.

Result:

The screen displays a confirmation message.

- 4 Click yes.

END OF STEPS





16 Clear test history

Overview

Purpose “Clear test history” describes how to use the Clear Test History window. The system keeps a record of the last 25 tests. Use the Clear Test History window to delete records for a specific piece of equipment or for a range of equipment.

Window location *Maintenance > Clear Test History Records*

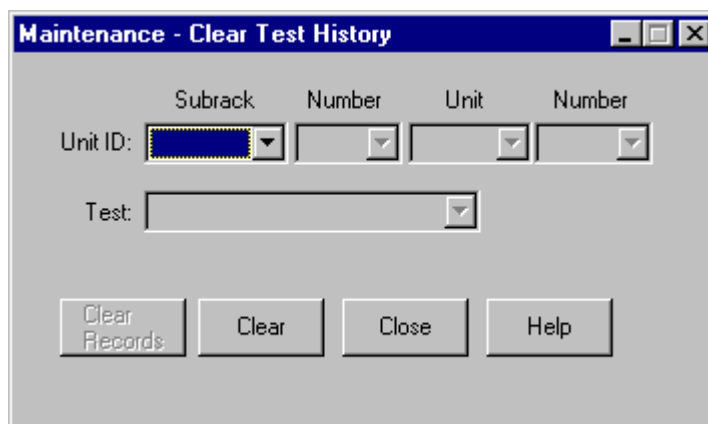
Organisation “Clear test history” is organised as follows:

- “Clear Test History window description” (16-2)
- “Clearing test records” (16-3)



Clear Test History window description

Illustration The following illustration shows the Clear Test History window.



Field descriptions The Clear Test History window has the following fields.

Field name	Description
Unit ID	The Unit ID field specifies the physical location of the unit that was tested.
Test	The Test field specifies the name of the test (BSSU Optical Loopback, Checksum, BCLAN...) that the system executed.



Clearing test records

Procedure

- 1 Go to the Clear Test History Records window at *Maintenance > Clear Test History Records*.
-

- 2 Select the Unit ID.

Use wildcards for less-specific address requests.

- 3 Select the test you want to clear in the Test field.

Result:

If you selected a wildcard (ALL) in the Unit ID field, the system automatically selects a wildcard in the Test field.

- 4 Click Clear Records.

END OF STEPS





17 Automatic laser shutdown

Overview

Purpose “Automatic laser shutdown” describes how to use the Automatic Laser Shutdown window. Use the Automatic Laser Shutdown window to manually restart the laser, or to manually restart the laser for test.

Window location *Maintenance > Automatic Laser Shutdown*

Organisation “Automatic laser shutdown” is organised as follows:

- “About automatic laser shutdown” (17-2)
- “Restart modes” (17-3)
- “Automatic Laser Shutdown window description” (17-4)
- “Restarting a laser” (17-5)



About automatic laser shutdown

Purpose of automatic laser shutdown

The system automatically shuts down the transmitting laser in an STM-4 or STM-16 port unit as soon as the system detects an interruption in the received optical signal. The interruption can be caused by a cable break or by disconnecting a transmission cable. The system shuts down the laser to prevent eye damage to maintenance personnel, and to prevent equipment damage caused by an optical surge.

About enabling and disabling automatic laser shutdown

Use the Port window at *Provision > Transmission > Port* to enable or disable the automatic laser shutdown feature. The Query Port button on the Automatic Laser Shutdown window will open the Port window.

When does automatic laser shutdown occur?

Whenever the system continually detects a signal loss in the received signal for half a second on an STM-4 or STM-16 port, the system will shut down the laser output. If the system detects continuous signal loss for half a second, the system issues the shutdown command. The system automatically restarts the laser. You can also manually restart the laser.



Restart modes

Description of restart modes

The following table describes how each of the restart modes works.

Restart mode	Description
Automatic	Restart is automatic. The laser will remain in the off state for approximately 1 minute. After this waiting period, the system will switch on the laser for approximately 2 seconds. The laser will remain on if the received signal loss defect clears. If there are problems, the cycle continues.
Manual	You can manually restart the laser before 1 minute has elapsed. Like during an automatic restart, the system performs a 2-second transmission test during this restart, and if the received loss of signal clears, the signal is restored. If there are problems, the automatic restart cycle continues.
Manual restart for test	Manual restart for test works the same as manual restart, except that the system will switch on the laser for approximately 90 seconds, instead of 2 seconds. The system will restore the laser if during this period the signal is transmitted properly without experiencing another signal loss of half a second or more. If there are problems, the automatic restart cycle continues.

Notes:

1. The system transmits Alarm Indication Signal (AIS) while the received signal loss persists. When the ALS feature is enabled, AIS remains on for 3 seconds after the received signal loss clears. When the ALS feature is disabled, AIS stops as soon as the received signal loss clears.



Automatic Laser Shutdown window description

Illustration The following illustration shows the Automatic Laser Shutdown window.



Field descriptions The Automatic Laser Shutdown window has the following fields.

Field name	Description
Port ID	The Port ID fields specify the physical location of a port. For a description of the Port ID options, see “About physical layer addresses” (5-3).



Restarting a laser

Procedure

- 1** Go to the Automatic Laser Shutdown window at *Maintenance > Automatic Laser Shutdown*.

- 2** Select the STM-4 or STM-16 Port ID.

- 3** Press either Manual Restart or Manual Restart for Test.

Reference:

For more information about the functions of these buttons, see “Restart modes” (17-3).

END OF STEPS





18 Database backups

Overview

Purpose “Database backups” describes how to use the Backup Database window. Use the Backup Database command on the Utilities menu to copy the contents of the system database onto a Magneto Optical (MO) disk.

Organisation “Database backups” is organised as follows:

- “Backup Database window” (18-2)
- “Backing up the system database” (18-3)



Backup Database window

Purpose Use the Backup Database command on the Utilities menu to copy the contents of the system database onto a Magneto Optical (MO) disk.

Window location *Utilities > Backup Database*

Illustration The following illustration shows an example of the Backup Database window.



□

Backing up the system database

Procedure

- 1 Insert a Magneto Optical (MO) disk that is *not* write protected into the magneto optical drive in the Main Controller subrack.

Reference:

For more information, see “MO disks” (2-6).

- 2 Go to the Utilities menu.
-

- 3 Select Backup Database.

Result:

A window with the following text appears: Database backup requires an unprotected disk in the MO drive. This disk will be overwritten with the current data. Do you wish to continue?

- 4 Click Yes.

Result:

Wait until the command completes. You will know that the command has completed when the busy cursor disappears.

- 5 Remove the MO disk from the drive.
-

- 6 Write the date on the MO disk, and store it in a safe place.

END OF STEPS





19 Fibre assignments

Overview

Purpose “Fibre assignments” describes the Fibre Assignments window. Use the Fibre Assignments window to query the expected and received fibre IDs for all fibre-optic cables that terminate on BSIUs, BSSUs, and OLU.

Window location *Utilities > Fibre Assignments*

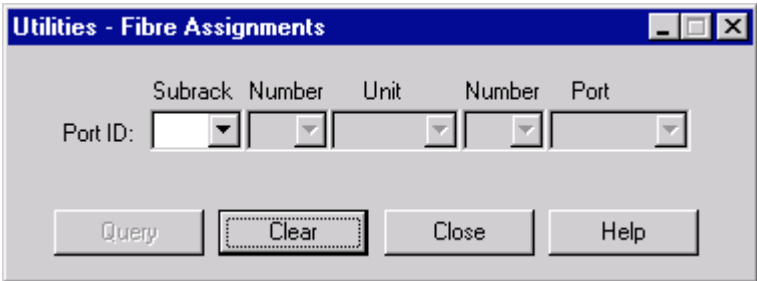
Organisation “Fibre assignments” is organised as follows:

- [“Fibre Assignments window description” \(19-2\)](#)
- [“Fibre-optic cable assignments” \(19-3\)](#)
- [“Querying fibre-optic cable assignments” \(19-4\)](#)
- [“Fibre Assignments query results” \(19-5\)](#)



Fibre Assignments window description

Illustration The following illustration shows the Fibre Assignments window.



Field description The Fibre Assignments window has the following field.

Field name	Description
Port ID	The Port ID field specifies the physical location of a fibre-optic cable connection.

Related topics For more information, see one of the following topics:

- “About the main application window” (4-10)
- “Fibre-optic cable assignments” (19-3)



Fibre-optic cable assignments

For a 256 system The following table lists fibre-optic cable addresses and the associated cable connections for a 256 system.

Fibre address	Fibre connection
MS-3-OLU-{1-4, ALL}-BSFI{1-5, ALL}	From BSSU to OLU
MS-3-BSSU-{1-10, ALL}-BSFI{W, P}	From OLU to BSSU
MS-3-BSSU-{1-10, ALL}-ECI{1-8}	From BSIU to BSSU
MS-3-BSSU-{1-10, ALL}-ALL	From OLU to BSSU and BSIU to BSSU
{PSA, PSC}-{4-11}-BSIU-{1-10, ALL}-ECI{1, 2, ALL}	From BSSU to BSIU

For a 512 system The following table lists fibre-optic cable addresses and the associated cable connections for a 512 system.

Fibre address	Fibre connection
MS-3-OLU-{1-4, ALL}-BSFI{1-5, ALL}	From BSSU to OLU
MS-3-BSSU-{1-10, ALL}-BSFI{W, P}	From OLU to BSSU
MS-3-BSSU-{1-10, ALL}-ECI{1-16}	From BSIU to BSSU
MS-3-BSSU-{1-10, ALL}-ALL	From OLU to BSSU and BSIU to BSSU
PSA-{4-19}-BSIU-{1-10, ALL}-ECI{1, 2, ALL}	From BSSU to BSIU
PSC-{4-19}-BSIU-{1-10, ALL}-ECI{1-4, ALL}	From BSSU to BSIU



Querying fibre-optic cable assignments

Procedure

- 1 Go to the Fibre Assignments window at *Utilities > Fibre Assignments*.
-

- 2 Select a Port ID.
-

- 3 Click Query.

Result:

If the Received Fibre ID and Expected Fibre ID values are different, contact technical support.

Reference:

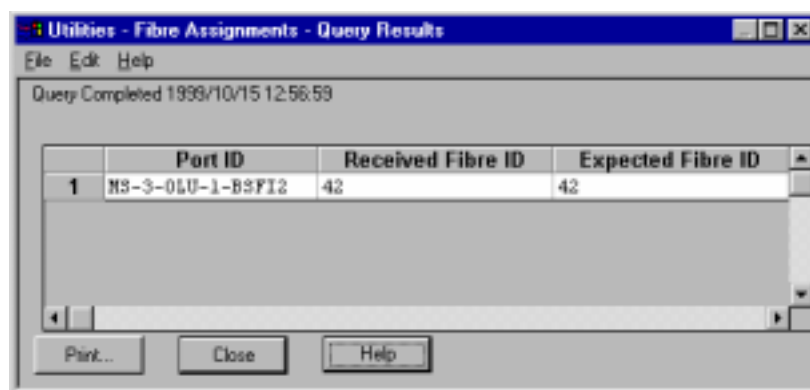
For diagrams of the fibre connections, see the *Installation Assembly Manual*.

END OF STEPS



Fibre Assignments query results

Illustration Use the following illustration only as an example of query results for the Fibre Assignments window.



Important! The data displayed on this screen may *not* be typical.

Results field descriptions The following information appears in the Fibre Assignments Query Results window.

Column	Description
Port ID	Displays the requested port ID.
Received Fibre ID	Displays the fibre ID that the system actually received. The value in this field should be identical to the value in the Expected Fibre ID field.
Expected Fibre ID	Displays the fibre ID that the system expected to receive. The value in this field should be identical to the value in the Received Fibre ID field.

Related topics For more information, see one of the following topics:

- “About the main application window” (4-10)
- “Fibre-optic cable assignments” (19-3)





20 Test access

Overview

- Purpose** “Test access” contains the following information:
- General information about test access connections
 - Step-by-step procedures for establishing and removing test access connections

- Organisation** “Test access” is organised as follows:
- “Background information” (20-2)
 - “MONE mode” (20-6)
 - “MONF mode” (20-10)
 - “MONEF mode” (20-14)
 - “SPLTA mode” (20-20)
 - “SPLTB mode” (20-27)
 - “SPLTAB mode” (20-34)
 - “SPLTE mode” (20-44)
 - “SPLTF mode” (20-48)
 - “SPLTEF mode” (20-52)
 - “LOOPE mode” (20-59)
 - “LOOPF mode” (20-63)



Background information

Overview

Purpose This section provides background information needed to understand test access.

Organisation This section contains the following information:

- “Getting started” (20-3)
- “Test access concepts” (20-4)



Getting started

What do I need to begin?

To establish or remove a test access connection, you will need the following information and tools:

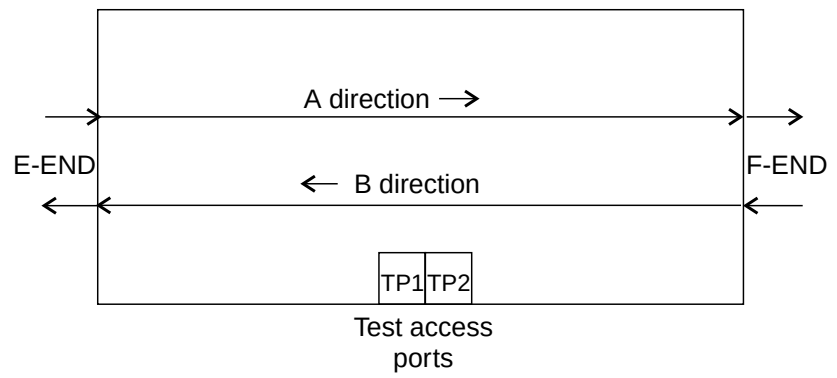
- Compliance with local operation procedures, including having access to an analyser and knowing how to use it
- Entity address of a test access port which consists of two adjacent idle ports
- TU-12, TU-3, AU-3, AU-4, or AU-4-4c address of the E-END
- TU-12, TU-3, AU-3, AU-4, or AU-4-4c address of the F-END



Test access concepts

- List of terms**
- A direction** The A direction is the direction in which the signal travels through the system from the E-END to the F-END, or the direction in a unidirectional cross connect.
- B direction** The B direction is the direction in which the signal travels through the system from the F-END to the E-END.
- E-END** E-END is an arbitrary designation used to distinguish one end of a unidirectional, bidirectional, idle (unmapped), or bridge cross connect as the signal travels through the system. You can establish test access at either the E-END or the F-END.
- F-END** F-END is an arbitrary designation used to distinguish the end opposite the E-END of a unidirectional, bidirectional, or bridge cross connect as the signal travels through the system. You can establish test access at either the E-END or the F-END.
- Idle** An output port is idle if the port is not cross connected to an input port.
- Loopback test access connection** A loopback test access connection loops back one end of a signal onto itself and bridges the connection to the test access port. Use loopback test access connections to test idle ports. LOOPE and LOOPF are loopback test access connections.
- Monitor test access connection** A monitor test access connection allows you to connect test equipment in parallel with a digital signal path while maintaining the digital transmission signal. Even though this test does *not* affect service, you will receive a confirmation notice from the user interface when you make a monitor test access connection. MONE, MONF, and MONEF are monitor test access connections.
- Split test access connection** A split test access connection splits the digital transmission path so that you can perform tests in both directions. SPLTA, SPLTB, SPLTAB, SPLTE, SPLTF, and SPLTEF are split test access connections.
- Test access ports TP1 and TP2** Test access ports TP1 and TP2 are the software addresses for the test access ports. Test access ports are located on the port units.
- UNEQ** The system sends an unequipped (UNEQ) signal from all ports that are *not* cross connected. During certain modes of test access, an UNEQ signal means that there is no cross-connected signal at the time of test access.

Test access conventions



MONE mode

Overview

Purpose This section contains information about the Monitor E (MONE) mode of test access.

Organisation This section contains the following information:

- [“About MONE mode” \(20-7\)](#)
- [“Establishing MONE mode” \(20-8\)](#)
- [“Disconnecting MONE mode” \(20-9\)](#)

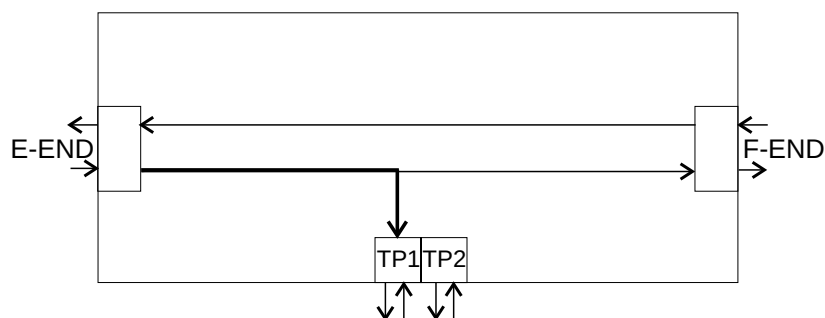


About MONE mode

What is MONE mode?

The MONE mode of test access does the following:

- Monitors transmission from the E-END
- Allows you to establish test access on an idle port, unidirectional cross connect, or bidirectional cross connect
- Uses one test access port
- Establishes a bridge from the E-END to the TP1 test access port
- Reads the incoming signal in direction A



Establishing MONE mode

Procedure

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.

- 2** Click Uni-Directional as the Cross Connect Type.

- 3** Click the appropriate Signal Type.

- 4** Select the E-END address in the From ID fields (Port ID and Signal ID).

- 5** Select the TP1 address in the To ID fields.

- 6** Click Connect.

END OF STEPS



Disconnecting MONE mode

- Procedure**
- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
.....
 - 2** Click Uni-Directional as the Cross Connect Type.
.....
 - 3** Click the appropriate Signal Type.
.....
 - 4** Select the E-END address in the From ID fields.
.....
 - 5** Select the TP1 address in the To ID fields.
.....
 - 6** Click Disconnect.
.....
- END OF STEPS



MONF mode

Overview

Purpose This section contains information about the Monitor F (MONF) mode of test access.

Organisation This section contains the following information:

- [“About MONF mode” \(20-11\)](#)
- [“Establishing MONF mode” \(20-12\)](#)
- [“Disconnecting MONF mode” \(20-13\)](#)

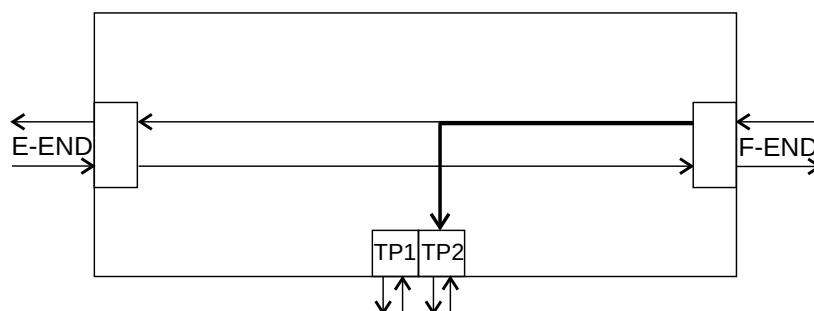


About MONF mode

What is MONF mode?

The MONF mode of test access does the following:

- Monitors transmission from the F-END
- Allows you to establish test access on a bidirectional cross connect
- Uses one test access port
- Establishes a bridge from the F-END to the TP2 test access port
- Reads the incoming signal in direction B



□

Establishing MONF mode

Procedure

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.

- 2** Click Uni-Directional as the Cross Connect Type.

- 3** Click the appropriate Signal Type.

- 4** Select the F-END address in the From ID fields (Port ID and Signal ID).

- 5** Select the TP2 address in the To ID fields.

- 6** Click Connect.

END OF STEPS



Disconnecting MONF mode

Procedure

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.

- 2** Click Uni-Directional as the Cross Connect Type.

- 3** Click the appropriate Signal Type.

- 4** Select the F-END address in the From ID fields.

- 5** Select the TP2 address in the To ID fields.

- 6** Click Disconnect.

END OF STEPS



MONEF mode

Overview

Purpose This section contains information about the Monitor EF (MONEF) mode of test access.

Organisation This section contains the following information:

- [“About MONEF mode” \(20-15\)](#)
- [“Establishing MONEF mode” \(20-16\)](#)
- [“Disconnecting MONEF mode” \(20-18\)](#)

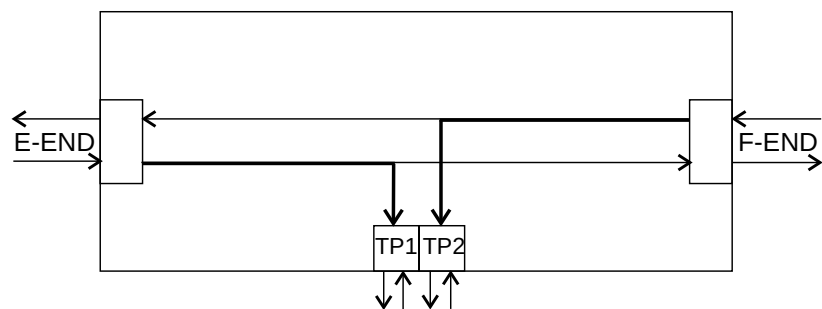


About MONEF mode

What is MONEF mode?

The MONEF mode of test access does the following:

- Monitors transmission from the E-END and the F-END
- Allows you to establish test access on bidirectional cross connects
- Uses both TP1 and TP2 test access ports
- Establishes a bridge from the E-END to the TP1 test access port and from the F-END to the TP2 test access port
- Reads the incoming signals in directions A and B



Establishing MONEF mode

Procedure overview The following list describes the procedures needed to establish a MONEF mode test access connection:

- “Establish E-END to TP1” (20-16)
- “Establish F-END to TP2” (20-16)

Establish E-END to TP1 Do the following to establish the E-END to TP1 portion of the MONEF test access connection.

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.

- 2** Click Uni-Directional as the Cross Connect Type.

- 3** Click the appropriate Signal Type.

- 4** Select the E-END address in the From ID fields (Port ID and Signal ID).

- 5** Select the TP1 address in the To ID fields.

- 6** Click Connect.

END OF STEPS

Establish F-END to TP2 Do the following to establish the F-END to TP2 portion of the MONEF test access connection.

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.

- 2** Click Uni-Directional as the Cross Connect Type.

- 3** Click the appropriate Signal Type.

- 4** Select the F-END address in the From ID fields.

.....
5 Select the TP2 address in the To ID fields.

.....
6 Click Connect.

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



Disconnecting MONEF mode

Procedure overview The following list describes the procedures needed to disconnect a MONEF mode test access connection:

- “Disconnect F-END to TP2” (20-18)
- “Disconnect E-END to TP1” (20-18)

Disconnect F-END to TP2 Do the following to disconnect the F-END to TP2 portion of the MONEF test access connection.

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.

- 2** Click Uni-Directional as the Cross Connect Type.

- 3** Click the appropriate Signal Type.

- 4** Select the F-END address in the From ID fields (Port ID and Signal ID).

- 5** Select the TP2 address in the To ID fields.

- 6** Click Disconnect.

END OF STEPS

Disconnect E-END to TP1 Do the following to disconnect the E-END to TP1 portion of the MONEF test access connection.

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.

- 2** Click Uni-Directional as the Cross Connect Type.

- 3** Click the appropriate Signal Type.

- 4** Select the E-END address in the From ID fields.

.....

5 Select the TP1 address in the To ID fields.

.....

6 Click Disconnect.

.....

E N D O F S T E P S

.....



SPLTA mode

Overview

Purpose This section contains information about the Split A (SPLTA) mode of test access.

Organisation This section contains the following information:

- [“About SPLTA mode” \(20-21\)](#)
- [“Establishing SPLTA mode” \(20-22\)](#)
- [“Disconnecting SPLTA mode” \(20-25\)](#)



About SPLTA mode

What is SPLTA mode?

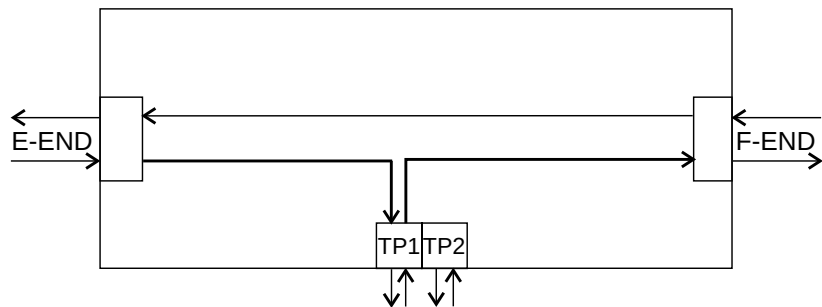
The SPLTA mode of test access does the following:

- Splits the transmission line from the E-END to the F-END
- Allows you to establish test access on a unidirectional, bidirectional, or bridge cross connect
- Uses the first test access port (TP1)
- Tests in the A direction

What type of test access connection does SPLTA establish?

When you establish a SPLTA mode of test access, you will be disconnecting the original cross connection and establishing the following:

- A unidirectional cross connect from the E-END to the TP1 test access port
- A unidirectional cross connect from the TP1 test access port to the F-END
- A unidirectional cross connect from the F-END to the E-END



Establishing SPLTA mode



This test access mode affects service.

- Procedure overview**
- The following list describes the procedures needed to establish a SPLTA mode test access connection:
- “Establish TP1 to F-END” (20-22)
 - “Establish E-END to TP1” (20-23)

Establish TP1 to F-END

Do the following to establish the TP1 to F-END portion of the SPLTA test access connection.

- 1

Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.
- 2

Click Uni-Directional in the Cross Connect Type field.
- 3

Click the appropriate Signal Type.
- 4

Select the E-END address in the From ID fields.
- 5

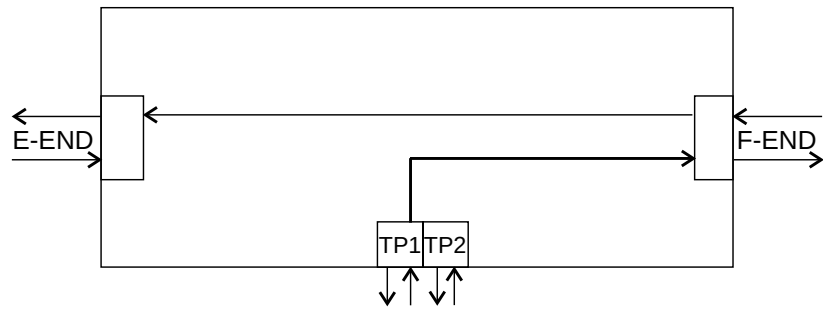
Select the F-END address in the To ID fields.
- 6

Select the TP1 address in the New From ID fields.
- 7

Click Roll.

END OF STEPS

Result

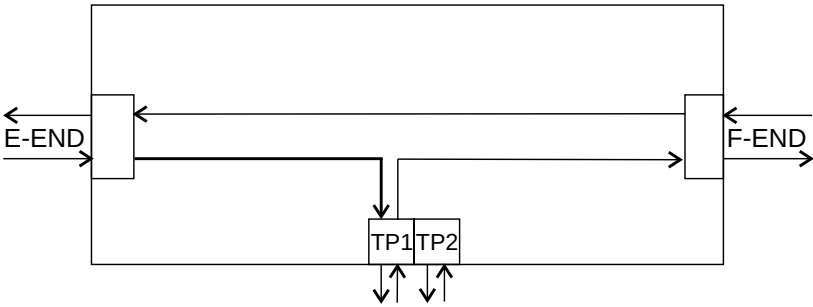


Establish E-END to TP1 Do the following to establish the E-END to TP1 portion of the SPLTA test access connection.

- 1 Go to the Cross Connect window.
- 2 Click Uni-Directional in the Cross Connect Type field.
- 3 Click the appropriate Signal Type.
- 4 Select the E-END address in the From ID fields.
- 5 Select the TP1 address in the To ID fields.
- 6 Click Connect.

END OF STEPS

Result



□

Disconnecting SPLTA mode

Procedure overview The following list describes the procedures needed to disconnect a SPLTA mode test access connection:

- “Disconnect E-END to TP1” (20-25)
- “Establish E-END to F-END” (20-25)

Disconnect E-END to TP1 Do the following to disconnect the E-END to TP1 portion of the SPLTA test access connection.

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.

- 2** Click Uni-Directional in the Cross Connect Type field.

- 3** Click the appropriate Signal Type.

- 4** Select the E-END address in the From ID fields.

- 5** Select the TP1 address in the To ID fields.

- 6** Click Disconnect.

END OF STEPS

Establish E-END to F-END Do the following to establish the E-END to F-END cross connection.

- 1** Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.

- 2** Click Uni-Directional in the Cross Connect Type field.

- 3** Click the appropriate Signal Type.

- 4** Select the TP1 address in the From ID fields.

.....
5 Select the F-END address in the To ID fields.

.....
6 Select the E-END address in the New From ID fields.

.....
7 Click Roll.

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



SPLTB mode

Overview

Purpose This section contains information about the Split B (SPLTB) mode of test access.

Organisation This section contains the following information:

- [“About SPLTB mode” \(20-28\)](#)
- [“Establishing SPLTB mode” \(20-29\)](#)
- [“Disconnecting SPLTB mode” \(20-32\)](#)



About SPLTB mode

What is SPLTB mode?

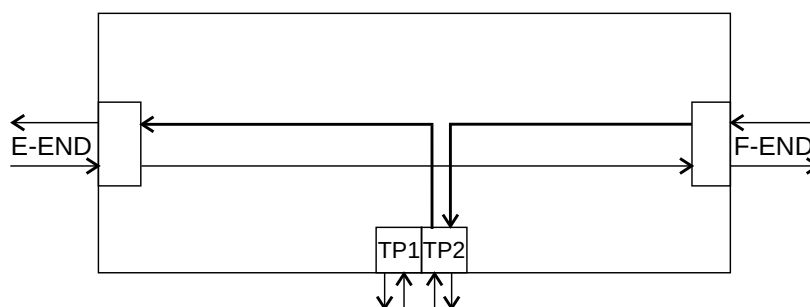
The SPLTB mode of test access does the following:

- Splits the transmission line from the F-END to the E-END
- Allows you to establish test access on a bidirectional cross connect
- Uses the second test access port (TP2)
- Tests in the B direction

What type of test access connection does SPLTB establish?

When you establish a SPLTB mode of test access, you will be disconnecting the original cross connection and establishing the following:

- A unidirectional cross connect from the F-END to the TP2 test access port
- A unidirectional cross connect from the TP2 test access port to the E-END
- A unidirectional cross connect from the E-END to the F-END



□

Establishing SPLTB mode



CAUTION

This test access mode affects service.

Procedure overview The following list describes the procedures needed to establish a SPLTB mode test access connection:

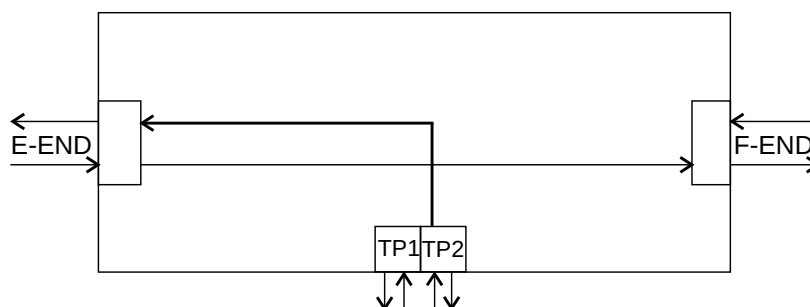
- “Establish TP2 to E-END” (20-29)
- “Establish F-END to TP2” (20-30)

Establish TP2 to E-END Do the following to establish the TP2 to E-END portion of the SPLTB test access connection.

- 1** Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.
- 2** Click Uni-Directional in the Cross Connect Type field.
- 3** Click the appropriate Signal Type.
- 4** Select the F-END address in the From ID fields.
- 5** Select the E-END address in the To ID fields.
- 6** Select the TP2 address in the New From ID fields.
- 7** Click Roll.

END OF STEPS

Result

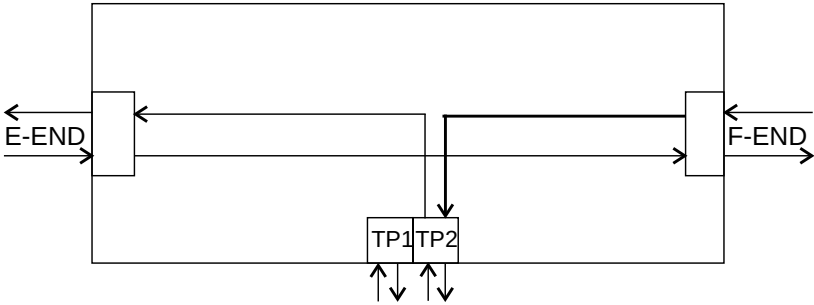


Establish F-END to TP2 Do the following to establish the F-END to TP2 portion of the SPLTB test access connection.

- 1 Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2 Click Uni-Directional in the Cross Connect Type field.
- 3 Click the appropriate Signal Type.
- 4 Select the F-END address in the From ID fields.
- 5 Select the TP2 address in the To ID fields.
- 6 Click Connect.

END OF STEPS

Result



□

Disconnecting SPLTB mode

Procedure overview The following list describes the procedures needed to disconnect a SPLTB mode test access connection:

- “Disconnect F-END to TP2” (20-32)
- “Establish F-END to E-END” (20-32)

Disconnect F-END to TP2 Do the following to disconnect the E-END to TP1 portion of the SPLTB test access connection.

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.

- 2** Click Uni-Directional in the Cross Connect Type field.

- 3** Click the appropriate Signal Type.

- 4** Select the F-END address in the From ID fields.

- 5** Select the TP2 address in the To ID fields.

- 6** Click Disconnect.

END OF STEPS

Establish F-END to E-END Do the following to establish the F-END to E-END cross connection.

- 1** Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.

- 2** Click Uni-Directional in the Cross Connect Type field.

- 3** Click the appropriate Signal Type.

- 4** Select the TP2 address in the From ID fields.

.....

5 Select the E-END address in the To ID fields.

.....

6 Select the F-END address in the New From ID fields.

.....

7 Click Roll.

.....

END OF STEPS



SPLTAB mode

Overview

Purpose This section contains information about the Split AB (SPLTAB) mode of test access.

Organisation This section contains the following information:

- [“About SPLTAB mode” \(20-35\)](#)
- [“Establishing SPLTAB mode” \(20-36\)](#)
- [“Disconnecting SPLTAB mode” \(20-41\)](#)



About SPLTAB mode

What is SPLTAB mode?

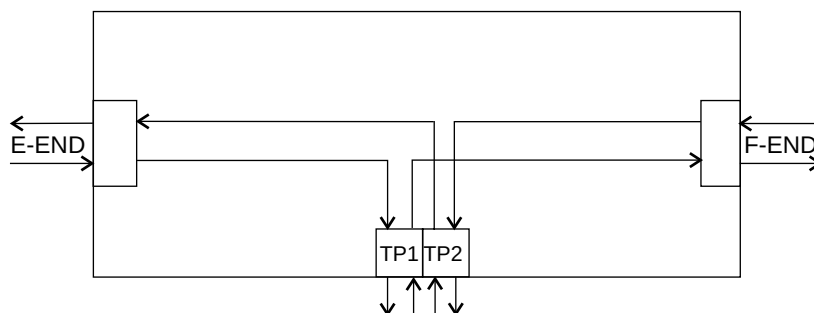
The SPLTAB mode of test access does the following:

- Splits the transmission line from the E-END to the F-END and the transmission line from the F-END to the E-END
- Allows you to establish test access on a bidirectional cross connect
- Tests in both the A and B directions

What type of test access connection does SPLTAB establish?

When you establish a SPLTAB mode of test access, you will be disconnecting the original cross connection and establishing the following:

- A unidirectional cross connect from the E-END to the TP1 test access port
- A unidirectional cross connect from the TP1 test access port to the F-END
- A unidirectional cross connect from the TP2 test access port to the E-END
- A unidirectional cross connect from the F-END to the TP2 test access port



Establishing SPLTAB mode



CAUTION

This test access mode affects service.

Procedure overview The following list describes the procedures needed to establish a SPLTAB mode test access connection:

- “Disconnect E-END to F-END” (20-36)
- “Establish TP1 to F-END” (20-37)
- “Establish E-END to TP1” (20-37)
- “Establish TP2 to E-END” (20-38)
- “Establish F-END to TP2” (20-39)

Disconnect E-END to F-END Do the following to disconnect the E-END to F-END cross connection.

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.

- 2** Click the appropriate cross connect type in the Cross Connect Type field.

- 3** Click the appropriate Signal Type.

- 4** Select the E-END address in the From ID fields.

- 5** Select the F-END address in the To ID fields.

- 6** Click Disconnect.

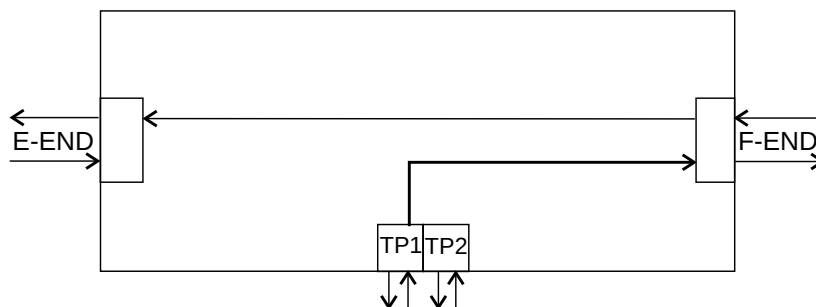
END OF STEPS

Establish TP1 to F-END Do the following to establish the TP1 to F-END portion of the SPLTAB test access connection.

- 1 Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.
- 2 Click Uni-Directional in the Cross Connect Type field.
- 3 Click the appropriate Signal Type.
- 4 Select the E-END address in the From ID fields.
- 5 Select the F-END address in the To ID fields.
- 6 Select the TP1 address in the New From ID fields.
- 7 Click Roll.

END OF STEPS

Result



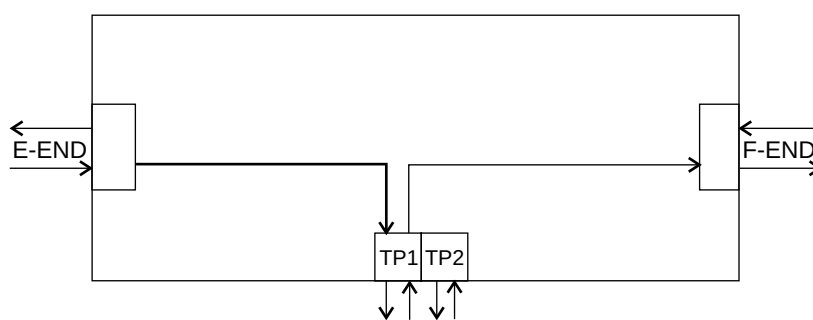
Establish E-END to TP1 Do the following to establish the E-END to TP1 portion of the SPLTAB test access connection.

- 1 Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2 Click Uni-Directional in the Cross Connect Type field.

- 3 Click the appropriate Signal Type.
- 4 Select the E-END address in the From ID fields.
- 5 Select the TP1 address in the To ID fields.
- 6 Click Connect.

END OF STEPS

Result



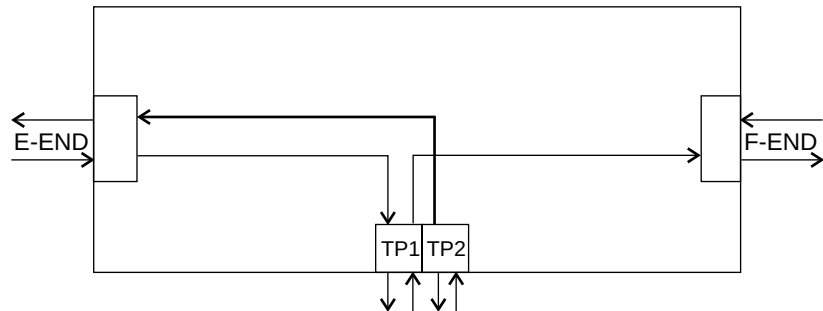
Establish TP2 to E-END Do the following to establish the TP2 to E-END portion of the SPLTAB test access connection.

- 1 Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.
- 2 Click Uni-Directional in the Cross Connect Type field.
- 3 Click the appropriate Signal Type.
- 4 Select the F-END address in the From ID fields.
- 5 Select the E-END address in the To ID fields.
- 6 Select the TP2 address in the New From ID fields.

7 Click Roll.

END OF STEPS

Result



Establish F-END to TP2 Do the following to establish the F-END to TP2 portion of the SPLTAB test access connection.

- 1** Go to the Cross Connect window.

- 2** Click Uni-Directional in the Cross Connect Type field.

- 3** Click the appropriate Signal Type.

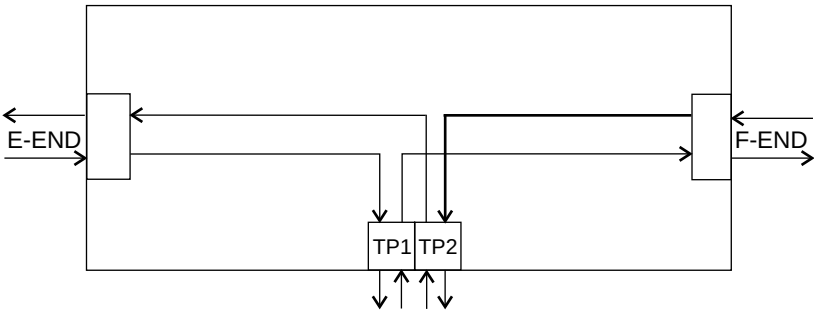
- 4** Select the F-END address in the From ID fields.

- 5** Select the TP2 address in the To ID fields.

- 6** Click Connect.

END OF STEPS

Result



□

Disconnecting SPLTAB mode

Procedure overview The following list describes the procedures needed to disconnect a SPLTAB mode test access connection:

- “Disconnect F-END to TP2” (20-41)
- “Establish F-END to E-END” (20-42)
- “Disconnect E-END to TP1” (20-42)
- “Establish E-END to F-END” (20-43)

Disconnect F-END to TP2 Do the following to disconnect the F-END to TP2 portion of the SPLTAB test access connection.

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2** Click Uni-Directional in the Cross Connect Type field.
- 3** Click the appropriate Signal Type.
- 4** Select the F-END address in the From ID fields.
- 5** Select the TP2 address in the To ID fields.
- 6** Click Disconnect.

END OF STEPS

Establish F-END to E-END

Do the following to establish the F-END to E-END cross connection.

- 1 Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.
- 2 Click Uni-Directional in the Cross Connect Type field.
- 3 Click the appropriate Signal Type.
- 4 Select the TP2 address in the From ID fields.
- 5 Select the E-END address in the To ID fields.
- 6 Select the F-END address in the New From ID fields.
- 7 Click Roll.

END OF STEPS

Disconnect E-END to TP1

Do the following to disconnect the E-END to TP1 portion of the SPLTAB test access connection.

- 1 Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2 Click Uni-Directional in the Cross Connect Type field.
- 3 Click the appropriate Signal Type.
- 4 Select the E-END address in the From ID fields.
- 5 Select the TP1 address in the To ID fields.
- 6 Click Disconnect.

END OF STEPS

Establish E-END to F-END

Do the following to establish the E-END to F-END cross connection.

- 1 Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.
- 2 Click Uni-Directional in the Cross Connect Type field.
- 3 Click the appropriate Signal Type.
- 4 Select the TP1 address in the From ID fields.
- 5 Select the F-END address in the To ID fields.
- 6 Select the E-END address in the New From ID fields.
- 7 Click Roll.

END OF STEPS



SPLTE mode

Overview

Purpose This section contains information about the Split E (SPLTE) mode of test access.

Organisation This section contains the following information:

- [“About SPLTE mode” \(20-45\)](#)
- [“Establishing SPLTE mode” \(20-46\)](#)
- [“Disconnecting SPLTE mode” \(20-47\)](#)



About SPLTE mode

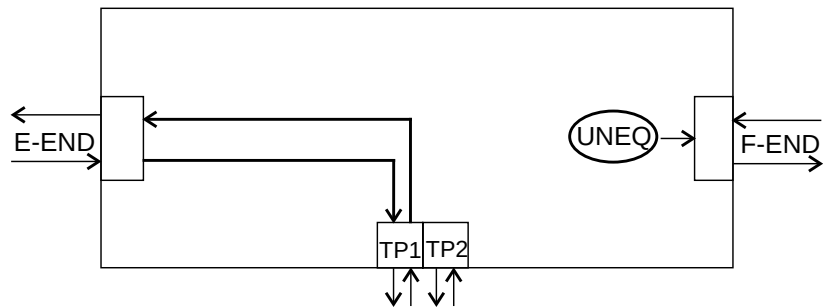
What is SPLTE mode?

The SPLTE mode of test access does the following:

- Splits off the transmission from the E-END
- Allows you to establish test access on an idle port or bidirectional cross connect
- Uses the TP1 test access port
- Sends an unequipped signal to the F-END

What type of test access connection does SPLTE establish?

When you establish a SPLTE mode of test access, you will be disconnecting the original cross connection and establishing a bidirectional cross connection from the E-END to the TP1 test access port.



Establishing SPLTE mode



CAUTION

This test access mode affects service.

- Procedure
- 1

Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.
- 2

Click Bi-Directional in the Cross Connect Type field.
- 3

Click the appropriate Signal Type.
- 4

Select the F-END address in the From ID fields (Port ID and Signal ID).
- 5

Select the E-END address in the To ID fields.
- 6

Select the TP1 address in the New From ID fields.
- 7

Click Roll.
- END OF STEPS
-

Disconnecting SPLTE mode

Procedure

- 1** Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.

- 2** Click Bi-Directional in the Cross Connect Type field.

- 3** Click the appropriate Signal Type.

- 4** Select the TP1 address in the From ID fields.

- 5** Select the E-END address in the To ID fields.

- 6** Select the F-END address in the New From ID fields.

- 7** Click Roll.

END OF STEPS



SPLTF mode

Overview

Purpose This section contains information about the Split F (SPLTF) mode of test access.

Organisation This section contains the following information:

- [“About SPLTF mode” \(20-49\)](#)
- [“Establishing SPLTF mode” \(20-50\)](#)
- [“Disconnecting SPLTF mode” \(20-51\)](#)



About SPLTF mode

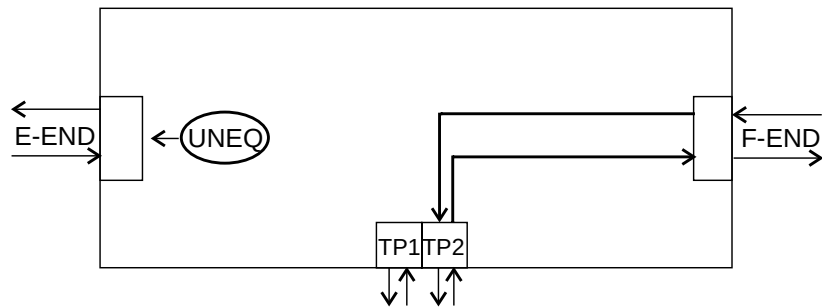
What is SPLTF mode?

The SPLTF mode of test access does the following:

- Splits off the transmission from the F-END
- Allows you to establish test access on an idle port or bidirectional cross connect
- Uses the TP2 test access port
- Sends an unequipped signal to the E-END

What type of test access connection does SPLTF establish?

When you establish a SPLTF mode of test access, you will be disconnecting the original cross connection and establishing a bidirectional cross connect from the F-END to the TP2 test access port.



Establishing SPLTF mode



CAUTION

This test access mode affects service.

- Procedure
- 1

Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.
- 2

Click Bi-Directional in the Cross Connect Type field.
- 3

Click the appropriate Signal Type.
- 4

Select the E-END address in the From ID fields (Port ID and Signal ID).
- 5

Select the F-END address in the To ID fields.
- 6

Select the TP2 address in the New From ID fields.
- 7

Click Roll.
- END OF STEPS
-

Disconnecting SPLTF mode

Procedure

- 1** Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.

- 2** Click Bi-Directional in the Cross Connect Type field.

- 3** Click the appropriate Signal Type.

- 4** Select the TP2 address in the From ID fields.

- 5** Select the F-END address in the To ID fields.

- 6** Select the E-END address in the New From ID fields.

- 7** Click Roll.

END OF STEPS



SPLTEF mode

Overview

Purpose This section contains information about the Split EF (SPLTEF) mode of test access.

Organisation This section contains the following information:

- [“About SPLTEF mode” \(20-53\)](#)
- [“Establishing SPLTEF mode” \(20-54\)](#)
- [“Disconnecting SPLTEF mode” \(20-57\)](#)



About SPLTEF mode

What is SPLTEF mode?

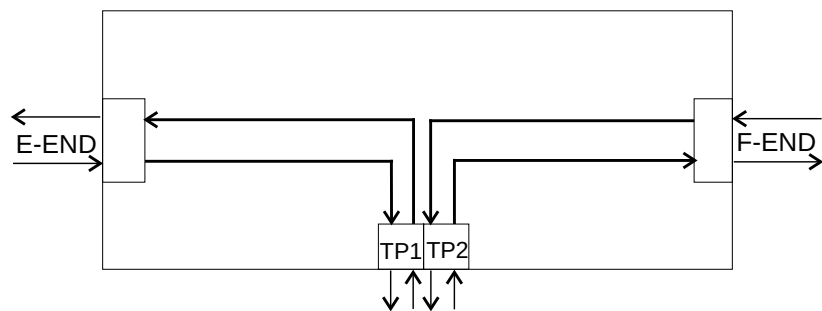
The SPLTEF mode of test access does the following:

- Splits off the transmission from the E-END and the F-END
- Allows you to establish test access on a bidirectional cross connect
- Uses both the TP1 and TP2 test access ports

What type of test access connection does SPLTEF establish?

When you establish a SPLTEF mode of test access, you will be disconnecting the original cross connection and establishing the following:

- A bidirectional cross connect from the E-END to the TP1 test access port
- A bidirectional cross connect from the F-END to the TP2 test access port



□

Establishing SPLTEF mode

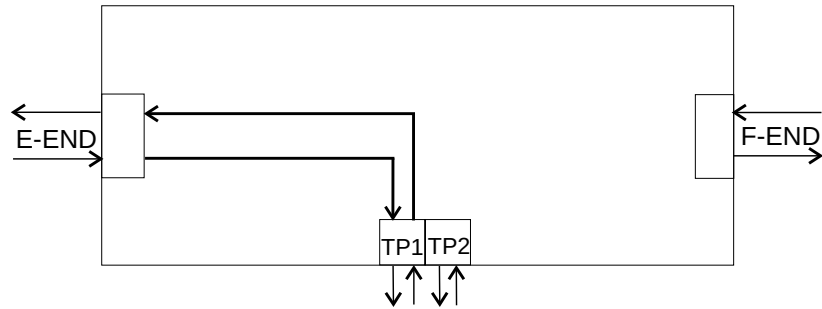
Procedure overview The following list describes the procedures needed to establish a SPLTEF mode test access connection:

- “Establish TP1 to E-END” (20-54)
- “Establish the F-END to TP2” (20-55)

Establish TP1 to E-END Do the following to establish the TP1 to E-END portion of the SPLTEF test access connection.

- 1** Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.
 - 2** Click Bi-Directional in the Cross Connect Type field.
 - 3** Click the appropriate Signal Type.
 - 4** Select the F-END address in the From ID fields (Port ID and Signal ID).
 - 5** Select the E-END address in the To ID fields.
 - 6** Select the TP1 address in the New From ID fields.
 - 7** Click Roll.
- END OF STEPS

Result

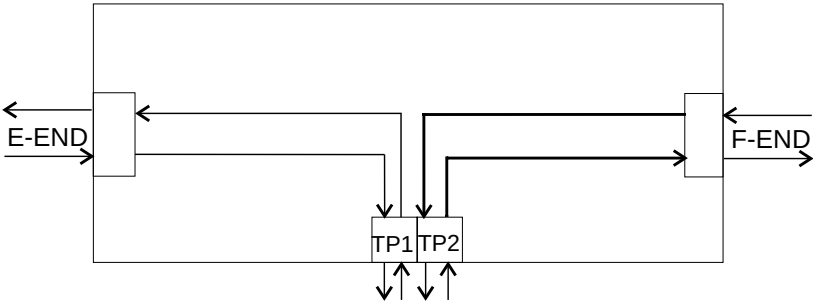


Establish the F-END to TP2 Do the following to establish the F-END to TP2 portion of the SPLTEF test access connection.

- 1 Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2 Click Bi-Directional in the Cross Connect Type field.
- 3 Click the appropriate Signal Type.
- 4 Select the F-END address in the From ID fields.
- 5 Select the TP2 address in the To ID fields.
- 6 Click Connect.

END OF STEPS

Result



□

Disconnecting SPLTEF mode

Procedure overview The following list describes the procedures needed to disconnect a SPLTEF mode test access connection:

- “Disconnect F-END to TP2” (20-57)
- “Establish F-END to E-END” (20-57)

Disconnect F-END to TP2 Do the following to disconnect the F-END to TP2 portion of the SPLTEF test access connection.

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.

- 2** Click Bi-Directional in the Cross Connect Type field.

- 3** Click the appropriate Signal Type.

- 4** Select the F-END address in the From ID fields.

- 5** Select the TP2 address in the To ID fields.

- 6** Click Disconnect.

END OF STEPS

Establish F-END to E-END Do the following to establish the F-END to E-END cross connection.

- 1** Go to the Connect Roll window at *Provision > Cross Connects > Connect Roll*.

- 2** Click Bi-Directional in the Cross Connect Type field.

- 3** Click the appropriate Signal Type.

- 4** Select the TP1 address in the From ID fields.

.....

5 Select the E-END address in the To ID fields.

.....

6 Select the F-END address in the New From ID fields.

.....

7 Click Roll.

.....

E N D O F S T E P S



LOOPE mode

Overview

Purpose This section contains information about the Loopback E (LOOPE) mode of test access.

Organisation This section contains the following information:

- [“About LOOPE mode” \(20-60\)](#)
- [“Establishing LOOPE mode” \(20-61\)](#)
- [“Disconnecting LOOPE mode” \(20-62\)](#)



About LOOPE mode

What is LOOPE mode?

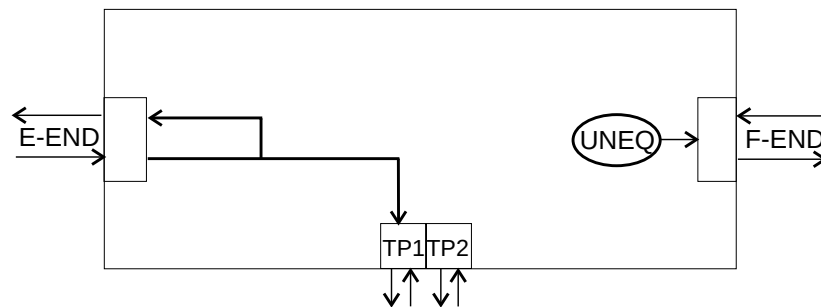
The LOOPE mode of test access does the following:

- Establishes a loopback test access connection at the E-END and monitors the loopback signal from the TP1 test access port
- Allows you to establish test access on an idle port
- Uses the TP1 test access port
- Sends an unequipped signal to the F-END

What type of test access connection does LOOPE establish?

When you establish a LOOPE mode of test access, you will be establishing the following:

- A unidirectional cross connect from the E-END to the TP1 test access port
- A loopback cross connect on the E-END



□

Establishing LOOPE mode

Procedure overview The following list describes the procedures needed to establish a LOOPE mode test access connection:

- “Establish loopback” (20-61)
- “Establish E-END to TP1” (20-61)

Establish loopback

- 1 Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2 Click Uni-Directional in the Cross Connect Type field.
- 3 Click the appropriate Signal Type.
- 4 Select the E-END address in *both* the From ID and To ID fields.
- 5 Click Connect.

END OF STEPS

Establish E-END to TP1

- 1 Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2 Click Uni-Directional in the Cross Connect Type field.
- 3 Click the appropriate Signal Type.
- 4 Select the E-END address in the From ID fields (Port ID and Signal ID).
- 5 Select the TP1 address in the To ID fields.
- 6 Click Connect.

END OF STEPS



Disconnecting LOOPE mode

- Procedure overview**
- The following list describes the procedures needed to disconnect a LOOPE mode test access connection:
- “Disconnect loopback” (20-62)
 - “Disconnect E-END to TP1” (20-62)

- Disconnect loopback**
- 1

Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2

Click Uni-Directional in the Cross Connect Type field.
- 3

Click the appropriate Signal Type.
- 4

Select the E-END address in *both* the From ID and To ID fields.
- 5

Click Disconnect.
- END OF STEPS

- Disconnect E-END to TP1**
- 1

Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2

Click Uni-Directional in the Cross Connect Type field.
- 3

Click the appropriate Signal Type.
- 4

Select the E-END address in the From ID fields.
- 5

Select the TP1 address in the To ID fields.
- 6

Click Disconnect.
- END OF STEPS



LOOPF mode

Overview

Purpose This section contains information about the Loopback F (LOOPF) mode of test access.

Organisation This section contains the following information:

- [“About LOOPF mode” \(20-64\)](#)
- [“Establishing LOOPF mode” \(20-65\)](#)
- [“Disconnecting LOOPF mode” \(20-66\)](#)



About LOOPF mode

What is LOOPF mode?

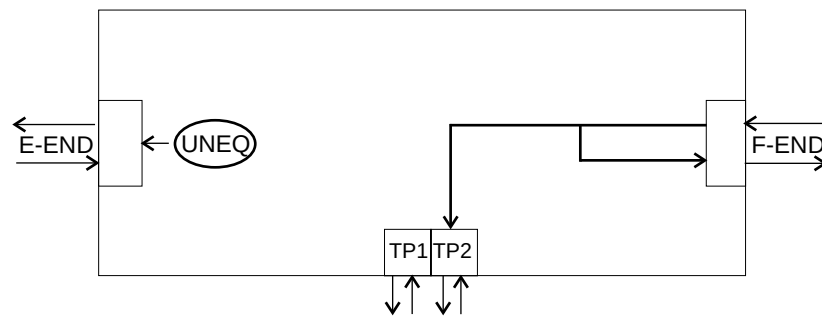
The LOOPF mode of test access does the following:

- Establishes a loopback test access connection at the F-END and monitors the loopback signal from the TP2 test access port
- Allows you to establish test access on an idle port
- Uses the TP2 test access port
- Sends an unequipped signal to the E-END

What type of test access connection does LOOPF establish?

When you establish a LOOPF mode of test access, you will be establishing the following:

- A unidirectional cross connect from the F-END to the TP2 test access port
- A loopback cross connect on the F-END



Establishing LOOPF mode

Procedure overview The following list describes the procedures needed to establish a LOOPF mode test access connection:

- “Establish loopback” (20-65)
- “Establish F-END to TP2” (20-65)

Establish loopback

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2** Click Uni-Directional in the Cross Connect Type field.
- 3** Click the appropriate Signal Type.
- 4** Select the F-END address in *both* the From ID and To ID fields.
- 5** Click Connect.

END OF STEPS

Establish F-END to TP2

- 1** Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2** Click Uni-Directional as the Cross Connect Type.
- 3** Click the appropriate Signal Type.
- 4** Select the F-END address in the From ID fields (Port ID and Signal ID).
- 5** Select the TP2 address in the To ID fields.
- 6** Click Connect.

END OF STEPS



Disconnecting LOOPF mode

Procedure overview The following list describes the procedures needed to disconnect a LOOPF mode test access connection:

- “Disconnect loopback” (20-66)
- “Disconnect F-END to TP2” (20-66)

Disconnect loopback

- 1 Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2 Click Uni-Directional in the Cross Connect Type field.
- 3 Click the appropriate Signal Type.
- 4 Select the F-END address in *both* the From ID and To ID fields.
- 5 Click Disconnect.

END OF STEPS

Disconnect F-END to TP2

- 1 Go to the Cross Connect window at *Provision > Cross Connects > Cross Connect*.
- 2 Click Uni-Directional as the Cross Connect Type.
- 3 Click the appropriate Signal Type.
- 4 Select the F-END address in the From ID fields.
- 5 Select the TP2 address in the To ID fields.
- 6 Click Disconnect.

END OF STEPS





21 Alarm clearing

Overview

Purpose “Alarm clearing” contains the following information:

- General information about clearing alarms
- Descriptions of specific alarms
- Step-by-step procedures for clearing alarms

Alarm list The following topics and alarms are described in “Alarm clearing”:

- “General alarm clearing” (21-4)
- “AUcAIS” (21-9)
- “AUcLOP” (21-12)
- “BCLANcEQ” (21-15)
- “BOOTcSW” (21-18)
- “CABLEcEQ” (21-21)
- “CABLEcTIM” (21-26)
- “DCNcCAALOF” (21-30)
- “DCNcMSNoNBR” (21-33)
- “DCNcREPAIR” (21-39)
- “DCNcRSNoNBR” (21-36)
- “DEGcEQ” (21-42)
- “DISKcFULL” (21-45)
- “FLTcEQ” (21-48)
- “FLTcSW” (21-88)
- “HPcDEG” (21-93)

- [“HPcPLM” \(21-96\)](#)
- [“HPcRDI” \(21-99\)](#)
- [“HPcTIM” \(21-102\)](#)
- [“HPcUNEQ” \(21-105\)](#)
- [“INTFcEQ” \(21-108\)](#)
- [“INVcCONF” \(21-112\)](#)
- [“INVcDPLL” \(21-115\)](#)
- [“INVcFPGA” \(21-119\)](#)
- [“LPcDEG” \(21-124\)](#)
- [“LPcRDI” \(21-127\)](#)
- [“LPcTIM” \(21-130\)](#)
- [“LPcUNEQ” \(21-133\)](#)
- [“MCLANcEQ” \(21-136\)](#)
- [“MDcIP{1–4}” \(21-141\)](#)
- [“MScAIS” \(21-146\)](#)
- [“MScDEG” \(21-149\)](#)
- [“MScFOP” \(21-152\)](#)
- [“MScRDI” \(21-155\)](#)
- [“OOScSW” \(21-158\)](#)
- [“POWcDEG” \(21-161\)](#)
- [“RScLOF” \(21-166\)](#)
- [“STMcLOS” \(21-169\)](#)
- [“SYNCcCCRF” \(21-172\)](#)
- [“SYNCcLTRF” \(21-178\)](#)
- [“SYNCcROOR” \(21-184\)](#)
- [“SYNCcSCF” \(21-187\)](#)
- [“SYNCcSCHO” \(21-190\)](#)
- [“SYNCcSTCOF” \(21-193\)](#)
- [“SYNCcSTCRF” \(21-198\)](#)
- [“TEMPcEQ” \(21-201\)](#)
- [“TUcAIS” \(21-204\)](#)
- [“TUcLOM” \(21-207\)](#)
- [“TUcLOP” \(21-210\)](#)
- [“UNIcEQ” \(21-213\)](#)
- [“VOLcDI” \(21-218\)](#)

- “VOLcREP” (21-221)
- “WUPcEQ” (21-224)



General alarm clearing

Overview

Purpose This section provides the general alarm-clearing procedure that you use before any other alarm-clearing procedure.

Organisation This section contains the following information:

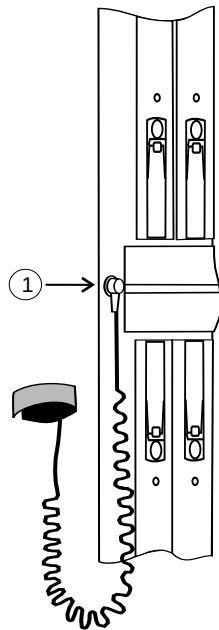
- “ESD caution” (21-5)
- “Alarm clearing sequence” (21-6)
- “General alarm clearing flowchart” (21-7)
- “General alarm clearing procedure” (21-8)



ESD caution

Caution Use a properly-grounded wrist strap whenever handling equipment. Using a wrist strap will dramatically reduce the chance of damaging the equipment by Electrostatic Discharge (ESD).

Every rack has a jack for plugging in a wrist strap.



Legend:

1. ESD jack

Related information For more information, see “About Electrostatic Discharge” (2-4).



Alarm clearing sequence

Clearing order for transmission and equipment alarms

Alarms from more than one failure category may exist at the same time. In situations such as this, clear the alarms by failure category in the following order:

1. Equipment failures
2. Transmission failures

Clearing order for prompt, deferred, and information alarms

Alarms of more than one severity level may exist at the same time. In situations such as this, clear alarms by severity level in the following order:

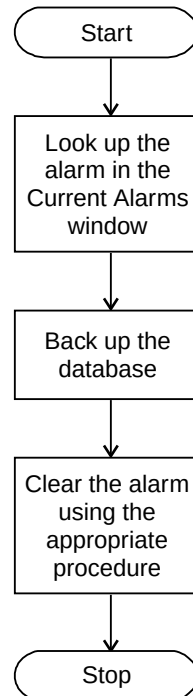
1. Prompt alarms
2. Deferred alarms
3. Information alarms



General alarm clearing flowchart

General alarm clearing flowchart

The following flowchart shows the general procedure for clearing an alarm.



□

General alarm clearing procedure

Alarm clearing actions



CAUTION

Do not remove any units without following the appropriate procedures. You could accidentally cause a service interruption, corrupt the hard disk, or power down a subrack and then have to reload the software from the Magneto Optical (MO) disks.

We recommend that you call technical support before attempting to replace a unit.

- 1 Look up the *failure condition* information (entity address, status, and so forth) by going to the View Current Alarms window at *Alarms > View Current Alarms*.
-

- 2 If you do not have a recent backup of the system, back up the database before proceeding. You must have a recent database backup in order to recover in the unlikely event of a system crash.

Reference:

For more information, see “Backing up the system database” (18-3).

- 3 If there is more than one alarm, clear the alarms in the proper order.

Reference:

For more information, see “Alarm clearing sequence” (21-6).

- 4 Clear the alarm by using the appropriate procedure for that particular alarm.

END OF STEPS



AUcAIS

Overview

Purpose This section contains information about AUcAIS alarms.

Organisation This section contains the following information:

- “AUcAIS description” (21-10)
- “Clearing AUcAIS alarms” (21-11)



AUcAIS description

Definition	Administrative Unit Alarm Indication Signal. The VC-3 or VC-4 payload signal has been replaced by AIS. The upstream equipment or an upstream function in the system has detected a defect which led to the insertion of AIS. This defect is detected by checking the AU-3, AU-4, or AU4-4c pointer bytes for an all “1”s pattern.
Alarm type	Transmission
Default severity level	You can change the severity levels. The default severity levels are as follows: • Prompt for failures that affect service • Information for failures that do not affect service
Local results	For Prompt alarms, a Prompt alarm indicator lights on the following: • User Panel • End-of-suite • Rack-top • Station For Information alarms, an Information alarm indicator on the User Panel lights. For Prompt and Information alarms, the red LED on the affected port unit flashes.
Remote results	The system does the following in the remote directions: • Generates an HPaRDI notification in the upstream direction • Inserts Alarm Indication Signal (AIS) into the transmission signal in the downstream direction



Clearing AUcAIS alarms

- Alarm clearing action** Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:
- A description of the problem
 - A request asking the administrator to examine the relevant equipment on the upstream end of the multiplex section



AUcLOP

Overview

Purpose This section contains information about AUcLOP alarms.

Organisation This section contains the following information:

- “AUcLOP description” (21-13)
- “Clearing AUcLOP alarms” (21-14)



AUcLOP description

Definition Administrative Unit (AU) Loss of Pointer. The system has not received a valid AU-3, AU-4, or AU4-4c pointer interpretation in the received signal. A unit failed in either the upstream equipment that generated the AU-3, AU-4, or AU4-4c pointer, or in the equipment that reported the alarm.

Alarm type Transmission

Default severity level You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected port unit flashes

Remote results The system does the following in the remote directions:

- Generates an HPaRDI notification in the upstream direction
- Inserts AIS into the transmission signal in the downstream direction



Clearing AUcLOP alarms

Alarm clearing action Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:

- A description of the problem
- A request asking the administrator to examine the relevant equipment on the upstream end of the multiplex section



BCLANcEQ

Overview

Purpose This section contains information about BCLANcEQ alarms.

Organisation This section contains the following information:

- “BCLANcEQ description” (21-16)
- “Clearing BCLANcEQ alarms” (21-17)



BCLANcEQ description

Definition A Board Controller Local Area Network (BCLAN) failure.

This alarm can be caused by any of the following:

- Equipment failure (a defective unit) in the BCLAN. Most likely, this would involve a defective SRC unit.
- Failures in several of the following units in the same subrack can also cause a BCLAN failure:
 - BSC
 - DTU
 - port unit
 - STU
- A LAN problem

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The SRC, STU, BSC, DTU, or the port unit LED is continuously lit.

Required equipment Obtain a new unit.



Clearing BCLANcEQ alarms

Clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
-

- 2 Perform a BCLAN diagnostic test.

Result:

If the BCLAN diagnostic test fails, an equipment alarm occurs.

Reference:

For the procedure, see “BCLAN procedure” (12-21).

- 3 Initialise the SRC.

Reference: For more information about initialising the SRC, see one of the following topics:

- “Removing an MS subrack SRC from service” (11-33)
 - “Removing a port subrack SRC from service” (11-34)
 - “Restoring an SRC to service” (11-35)
-

- 4 Reseat the unit.
-

- 5 Perform the BCLAN diagnostic test again.
-

- 6 If the alarm does not clear, replace the unit reporting the alarm by using the appropriate Fault-cEQ (FLTcEQ) procedure.

Example:

If the unit reporting the alarm is a DTU, use the procedure for clearing a FLTcEQ on a DTU.

Reference:

For the appropriate FLTcEQ unit-replacement procedure, see “FLTcEQ flowcharts and procedures” (21-48).

END OF STEPS



BOOTcSW

Overview

Purpose This section contains information about BOOTcSW alarms.

Organisation This section contains the following information:

- “BOOTcSW description” (21-19)
- “Clearing BOOTcSW alarms” (21-20)



BOOTcSW description

Definition A boot failure.

This alarm can be caused by one of the following:

- A hardware or software failure on a unit
- A defective LHU connection on the Main Controller

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red, or yellow if the unit is an MPU, LED on the affected unit is continuously lit.

Required equipment Obtain a new unit.



Clearing BOOTcSW alarms

Clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
-

- 2 Perform a warm start on the affected unit.

Reference:

For the procedure, see “Performing a warm start” (11-41).

- 3 If a warm start does not clear the alarm, cold start the unit.

Reference:

For the procedure, see “Performing a cold start” (11-42).



CAUTION

Do not remove any units without following the appropriate procedures. You could accidentally cause a service interruption, corrupt the hard disk, or power down a subrack and then have to reload the software from the Magneto Optical (MO) disks.

- 4 If you cannot cold start the unit, or if the alarm does not clear, replace the defective unit by using the appropriate Fault-cEQ (FLTcEQ) procedure.

Example:

If the unit reporting the alarm is an MPU, use the procedure for clearing a FLTcEQ on an MPU.

Reference:

To locate the appropriate FLTcEQ unit-replacement procedure, see “FLTcEQ flowcharts and procedures” (21-48).

- 5 Return any defective units to technical support.

Reference:

For more information, see “Procedure for returning defective equipment” (22-5).

END OF STEPS



CABLEcEQ

Overview

Purpose This section contains information about CABLEcEQ alarms.

Organisation This section contains the following information:

- “CABLEcEQ description” (21-22)
- “CABLEcEQ addresses” (21-23)
- “Clearing CABLEcEQ alarms” (21-24)



CABLEcEQ description

CABLEcEQ interfaces A CABLEcEQ alarm is associated with a fibre optic cable failure.

This alarm is applicable to the following interfaces:

- Bit Slice Fibre Interface (BSFI) — OLU to BSSU
- Equipment Core Interface (ECI) — BSSU to BSIU

Reasons for CABLEcEQ alarm A CABLEcEQ alarm can occur for any of the following reasons:

- Missing, defective, or loose cables
- Failure in one of the connected units
- Removal of a BSSU or a BSIU. In this case, the alarm should be temporary.
- System escalation of a warm start recovery to a cold start recovery. In this case, the alarm should be temporary.

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

Unit LEDs do not light for this alarm.

Required equipment Obtain one or more spare cables or connected units.



CABLEcEQ addresses

How CABLEcEQ and CABLEcTIM addresses are displayed

The following table displays both ends of an OLU to BSSU, and a BSSU to BSIU optical link. The system can detect a defect from either side of these optical interfaces. The unit that detects and reports the defect first is listed first.

Unit alarmed	Alarm displayed on
OLU or BSSU	MS-3-OLU-{1–4}-BSFI{1–5}
OLU or BSSU	MS-3-BSSU-{1–10}-BSFI{W,P}*
BSSU or BSIU	MS-3-BSSU-{1–10}-BSIU{1–8}
BSSU or BSIU	PSA-{4–11, 4–19}-BSIU-{1–10}-ECI{1, 2}
BSSU or BSIU	PSC-{4–11, 4–19}-BSIU-{1–10}-ECI{1–4}

* Use the following list to determine the OLU port on the BSSU unit:

- MS-3-BSSU-{1–5}-BSFIW = OLU-1
- MS-3-BSSU-{1–5}-BSFIP = OLU-3
- MS-3-BSSU-{6–10}-BSFIW = OLU-2
- MS-3-BSSU-{6–10}-BSFIP = OLU-4

Related topics

For more information about how to physically locate these cable interfaces, see any of the following:

- “Example of a fibre address” (5-19)
- *Installation Assembly Manual*



Clearing CABLEcEQ alarms

Purpose A CABLEcEQ alarm usually means that there is a missing, loose, or defective cable, between an OLU and BSSU, or between a BSSU and BSIU.

Clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
-

- 2 Verify that the cables are connected properly. Add missing cables as needed.

Reference: For more information about how to physically locate these cable interfaces, see any of the following:

- “How CABLEcEQ and CABLEcTIM addresses are displayed” (21-23)
 - “Example of a fibre address” (5-19)
 - *Installation Assembly Manual*
-

- 3 If the alarm did not clear, replace the cable.

Reference: For more information about replacing optical cables, see any of the following topics:

- “About cables” (3-2)
 - “Inserting a cable” (3-3)
 - “Removing a cable” (3-4)
-

- 4 If the alarm still did not clear, replace the unit reporting the alarm by using the appropriate Fault-cEQ (FLTcEQ) procedure.

Example:

If the unit reporting the alarm is an OLU, use the procedure for clearing a FLTcEQ on an OLU.

Reference:

To locate the appropriate FLTcEQ unit-replacement procedure, see “FLTcEQ flowcharts and procedures” (21-48).

- 5 If the alarm still did not clear, replace the unit at the other end of the cable.

-
- 6** If none of these actions correct the problem, call technical support.
-
- END OF STEPS
-
- ☐

CABLEcTIM

Overview

Purpose This section contains information about CABLEcTIM alarms.

Organisation This section contains the following information:

- “CABLEcTIM description” (21-27)
- “Differences between CABLEcEQ and CABLEcTIM alarms” (21-28)
- “Clearing CABLEcTIM alarms” (21-29)



CABLEcTIM description

Definition Cable Trace Identifier Mismatch. A CABLEcTIM alarm indicates an optical cable connection error.

This alarm can be caused by connecting a cable to the wrong port on any of the following units:

- BSIU
- BSSU
- OLU

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

Unit LEDs do not light for this alarm.



Differences between CABLEcEQ and CABLEcTIM alarms

Differences A CABLEcTIM alarm is similar to a CABLEcEQ alarm. The difference is that a CABLEcEQ alarm usually indicates a loose, missing, or defective cable. A CABLEcTIM usually indicates an incorrectly-connected cable.

Related topics For more information about how to physically locate these cable interfaces, see any of the following:

- “How CABLEcEQ and CABLEcTIM addresses are displayed” (21-23)
- “Example of a fibre address” (5-19)
- *Installation Assembly Manual*



Clearing CABLEcTIM alarms

Clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).

- 2 Perform a query on the *Utilities > Fibre Assignments* window to determine if the cable specified in the alarm is connected to the wrong port. If the Received Fibre ID and the Expected Fibre ID do not match, the cable is not connected properly.

- 3 Check the cabling to make sure the connections are correct.
Reference: For more information about how to physically locate these cable interfaces, see any of the following:
 - “How CABLEcEQ and CABLEcTIM addresses are displayed” (21-23)
 - “Example of a fibre address” (5-19)
 - *Installation Assembly Manual*

- 4 If the cables are connected properly, clear any alarms on the STU, BSC, BSSU, BSIU, or DTU by using the appropriate Fault-cEQ (FLTcEQ) procedure.
Reference: For more information, see one of the following topics:
 - “Clearing a FLTcEQ on a BSC or STU” (21-53)
 - “Clearing a FLTcEQ on a BSIU or BSSU” (21-57)
 - “Clearing a FLTcEQ on a DTU” (21-61)

- 5 If none of these actions correct the problem, call technical support.

END OF STEPS



DCNcCAALOF

Overview

Purpose This section contains information about DCNcCAALOF alarms.

Organisation This section contains the following information:

- “DCNcCAALOF description” (21-31)
- “Clearing DCNcCAALOF alarms” (21-32)



DCNcCAALOF description

Definition A DCNcCAALOF alarm is a Computed Area Address List overflow indication. CAAL is the union of the sets of Manual Area Addresses in one Area. If more than the maximum allowed number of addresses are present, the IS shall retain only the Area address numbers with the numerically-lowest Area address.

Alarm type Transmission

Default severity level You can change the severity level. The default severity level is Deferred for failures that do not affect service.

Local results A Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

A yellow LED on the affected MPU is continuously lit.



Clearing DCNcCAALOF alarms

Clearing actions

- 1 Check and correct the provisioning of the DCN MAAL in the related dSRCs while being careful to avoid exceeding the CAAL limitation (the default is no more than 3 per Area).
-

- 2 If the alarm still does not clear, call technical support.

END OF STEPS



DCNcMSNoNBR

Overview

Purpose This section contains information about DCNcMSNoNBR alarms.

Organisation This section contains the following information:

- “DCNcMSNoNBR description” (21-34)
- “Clearing DCNcMSNoNBR alarms” (21-35)



DCNcMSNoNBR description

Definition	A DCNcMSNoNBR alarm means that an MS DCC neighbor does not exist. The MS DCC channel can not be established or can be interrupted.
Alarm type	Transmission
Default severity level	You can change the severity level. The default severity level is Deferred for failures that do not affect service.
Local results	A Deferred alarm indicator lights on the following: • User Panel • End-of-suite • Rack-top • Station A yellow LED on the affected MPU is continuously lit.



Clearing DCNcMSNoNBR alarms

Clearing actions

- 1 Check and clear the transmission alarm (STM_LOS, RS_LOF, or MS_AIS) on the port.
- 2 Check and clear the transmission alarm (STM_LOS, RS_LOF, or MS_AIS) on the peer port.
- 3 Check and clear the equipment alarm (FLT_EQ, UNI_EQ, WUP_EQ, or BOOT_SW) on the port unit.
- 4 Check and clear the equipment alarm (FLT_EQ, UNI_EQ, WUP_EQ, or BOOT_SW) on the peer NE.
- 5 For a PSA subrack,
 1. Once more than one port in the same PU is enabled for DCC, check to see if all peer NEs are WaveStar AM1+ R3.0. If they are not, make a correction by configuring all the peer NEs as AM1+ R3.0, or only enable one port in that PU.
 2. Once the correct operation is achieved, (DCC slave MSP mode), check to see if uni-directional MSP is used. If it is, then change the provisioning to be bi-directional MSP.
- 6 If the alarm still does not clear, call technical support.

END OF STEPS



DCNcRSNoNBR

Overview

Purpose This section contains information about DCNcRSNoNBR alarms.

Organisation This section contains the following information:

- “DCNcRSNoNBR description” (21-37)
- “Clearing DCNcRSNoNBR alarms” (21-38)



DCNcRSNoNBR description

Definition A DCNcRSNoNBR alarm means that an RS DCC neighbor does not exist. The RS DCC channel can be established or can be interrupted.

Alarm type Transmission

Default severity level You can change the severity level. The default severity level is Deferred for failures that do not affect service.

Local results A Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

A yellow LED on the affected MPU is continuously lit.



Clearing DCNcRSNoNBR alarms

Clearing actions

- 1 Check and clear the transmission alarm (STM_LOS, RS_LOF, or MS_AIS) on the port.

- 2 Check and clear the transmission alarm (STM_LOS, RS_LOF, or MS_AIS) on the peer port.

- 3 Check and clear the equipment alarm (FLT_EQ, UNI_EQ, WUP_EQ, or BOOT_SW) on the subrack.

- 4 Check and clear the equipment alarm (FLT_EQ, UNI_EQ, WUP_EQ, or BOOT_SW) on the NE.

- 5 For a PSA subrack, once more than one port in the same PU is enabled for DCC, check to see if all peer NEs are WaveStar AM1+ R3.0. If they are not, make a correction by configuring all the peer NEs as AM1+ R3.0, or only enable one port in that PU.

- 6 If the alarm still does not clear, call technical support.

END OF STEPS



DCNcREPAIR

Overview

Purpose This section contains information about DCNcREPAIR alarms.

Organisation This section contains the following information:

- “DCNcREPAIR description” (21-40)
- “Clearing DCNcREPAIR alarms” (21-41)



DCNcREPAIR description

Definition	A DCNcREPAIR alarm is an IS-IS level 2 Area partition repair indication. If the customer designs and configures DCN for this feature, Area Partition Repair allows a level 1 tunnel to be built through the Level 2 subnetwork, thus rejoining the partitions of the level 1 Area in case that level 1 Area were to become divided with one or many DCN failures or some other sort of misconfiguration were to occur.
Alarm type	Transmission
Default severity level	You can change the severity level. The default severity level is Deferred for failures that do not affect service.
Local results	A Deferred alarm indicator lights on the following: • User Panel • End-of-suite • Rack-top • Station A yellow LED on the affected MPU is continuously lit.



Clearing DCNcREPAIR alarms

Clearing actions

- 1** Check to see if any "DCNcMSNoNBR" or "DCNcRSNoNBR" alarms exist in the same subrack. If these alarms exist, clear them. If this is not the case, go to Step 2.

- 2** Check the connection status to the external Q-LAN hub for the subrack, and fix any discovered connection failures in the cable connection or in the external Q-LAN hub. If there are no connection problems, go to Step 3.

- 3** If the alarm still does not clear, call technical support.

END OF STEPS



DEGcEQ

Overview

Purpose This section contains information about DEGcEQ alarms.

Organisation This section contains the following information:

- “DEGcEQ description” (21-43)
- “Clearing DEGcEQ alarms” (21-44)



DEGcEQ description

Definition A DEGcEQ alarm indicates a Degraded Equipment Failure condition caused by a degraded unit. A degraded unit is also referred to as a “defective” unit. A degraded unit is still functional.

The system generates this alarm against a degraded unit whenever a non-critical, system-generated, or user-initiated diagnostic test has failed.

Alarm type Equipment

Default severity level You can change the severity level. The default severity level is Deferred for failures that do not affect service.

Local results A Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red, or yellow if the unit is an MPU, LED on the affected unit is continuously lit.

Required equipment Obtain a new unit.



Clearing DEGcEQ alarms

Clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
.....
- 2 Perform a query using the Autonomous Messages window at *Reports > Autonomous Messages*. Select Diagnostic Test Completion Messages in the Message/Event Type field.
.....
- 3 Note the Device EID and Test of the failed diagnostic test that caused the alarm.
.....
- 4 Run the diagnostic test again.
.....



CAUTION

Do not remove any units without following the appropriate procedures. You could accidentally cause a service interruption, corrupt the hard disk, or power down a subrack and then have to reload the software from the Magneto Optical (MO) disks.

- 5 If the test did not pass, reseal or replace the unit by using the appropriate Fault-cEQ (FLTcEQ) procedure.

Example:

If the unit reporting the alarm is an MPU, use the procedure for clearing a FLTcEQ on an MPU.

Reference:

To locate the appropriate FLTcEQ unit-replacement procedure, see “FLTcEQ flowcharts and procedures” (21-48).

- 6 If the alarm still does not clear, call technical support.

END OF STEPS



DISKcFULL

Overview

Purpose This section contains information about DISKcFULL alarms.

Organisation This section contains the following information:

- “DISKcFULL description” (21-46)
- “Clearing DISKcFULL alarms” (21-47)



DISKcFULL description

Definition A DISKcFULL alarm is generated when an audit indicates that disk space is almost full (greater than 95% on one or more partitions).

Important! A DISKcFULL alarm is activated only on the Main Controller subrack.

Alarm type Equipment

Default severity level You can change the severity level. The default severity level is Deferred for failures that do not affect service.

Local results A Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

A yellow LED on the affected MPU is continuously lit.



Clearing DISKcFULL alarms

Clearing action Call technical support for assistance in clearing this alarm.



FLTcEQ

Overview

Purpose This section contains information about clearing Fault-cEQ (FLTcEQ) alarms.

FLTcEQ flowcharts and procedures Choose either the flowchart or the procedure for the unit with the FLTcEQ alarm.

Unit	Flowchart	Procedure
ARU	Not needed	“Clearing a FLTcEQ on an ARU, LHU, or PSP” (21-51)
BSC	“Flowchart for clearing a FLTcEQ on a BSC or STU” (21-52)	“Clearing a FLTcEQ on a BSC or STU” (21-53)
BSIU	“Flowchart for clearing a FLTcEQ on a BSIU or BSSU” (21-56)	“Clearing a FLTcEQ on a BSIU or BSSU” (21-57)
BSSU	“Flowchart for clearing a FLTcEQ on a BSIU or BSSU” (21-56)	“Clearing a FLTcEQ on a BSIU or BSSU” (21-57)
DTU	“Flowchart for clearing a FLTcEQ on a DTU” (21-60)	“Clearing a FLTcEQ on a DTU” (21-61)
FAN	“Flowchart for clearing a FLTcEQ on a fan in the MC subrack” (21-63)	“Clearing a FLTcEQ on a fan in the MC subrack” (21-64)
LHU	Not needed	“Clearing a FLTcEQ on an ARU, LHU, or PSP” (21-51)
IU	Not needed	“Clearing a FLTcEQ on an IU or an unprotected port unit” (21-67)
MPU	Not needed	“Clearing a FLTcEQ on an MPU” (21-69)

Unit	Flowchart	Procedure
MSU	Not needed	“Clearing a FLTcEQ on an MSU” (21-70)
OLU	“Flowchart for clearing a FLTcEQ on an OLU” (21-71)	“Clearing a FLTcEQ on an OLU” (21-72)
PSP	Not needed	“Clearing a FLTcEQ on an ARU, LHU, or PSP” (21-51)
SRC	“Flowchart for clearing a FLTcEQ on an SRC” (21-74)	“Clearing a FLTcEQ on an SRC” (21-75)
Port unit that is unprotected	Not needed	“Clearing a FLTcEQ on an IU or an unprotected port unit” (21-67)
Port unit that uses NTT MSP	“Flowchart for clearing a FLTcEQ on a port unit that uses NTT MSP” (21-80)	“Clearing a FLTcEQ on a port unit that uses NTT MSP” (21-81)
Port unit that uses ITU or ANSI MSP	“Flowchart for clearing a FLTcEQ on a port unit that uses SNCP, ITU MSP, or ANSI MSP” (21-84)	“Clearing a FLTcEQ on a port unit that uses SNCP, ITU MSP, or ANSI MSP” (21-85)
STM-1 electrical unit that uses 1:8 equipment protection	“Flowchart for clearing a FLTcEQ on an STM-1 electrical unit that uses 1:8 equipment protection” (21-76)	“Clearing a FLTcEQ on an STM-1 electrical unit that uses 1:8 equipment protection” (21-77)
STU	“Flowchart for clearing a FLTcEQ on a BSC or STU” (21-52)	“Clearing a FLTcEQ on a BSC or STU” (21-53)



FLTcEQ description

Definition A Fault-cEQ (FLTcEQ) alarm indicates an equipment failure associated with an ARU, BSC, BSIU, BSSU, DTU, FAN, IU, LHU, MPU, MSU, OLU, Power Supply (PSP), SRC, port unit, or STU.

The system generates a FLTcEQ alarm whenever a critical system-generated or user-initiated diagnostic test has failed.

Important! Call technical support before attempting to clear a FLTcEQ alarm on any equipment in the Main Controller (MC) subrack.

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red, or yellow if the unit is an MPU, LED on the affected unit is continuously lit.

Required equipment Obtain a new unit.



Clearing a FLTcEQ on an ARU, LHU, or PSP

Clearing actions

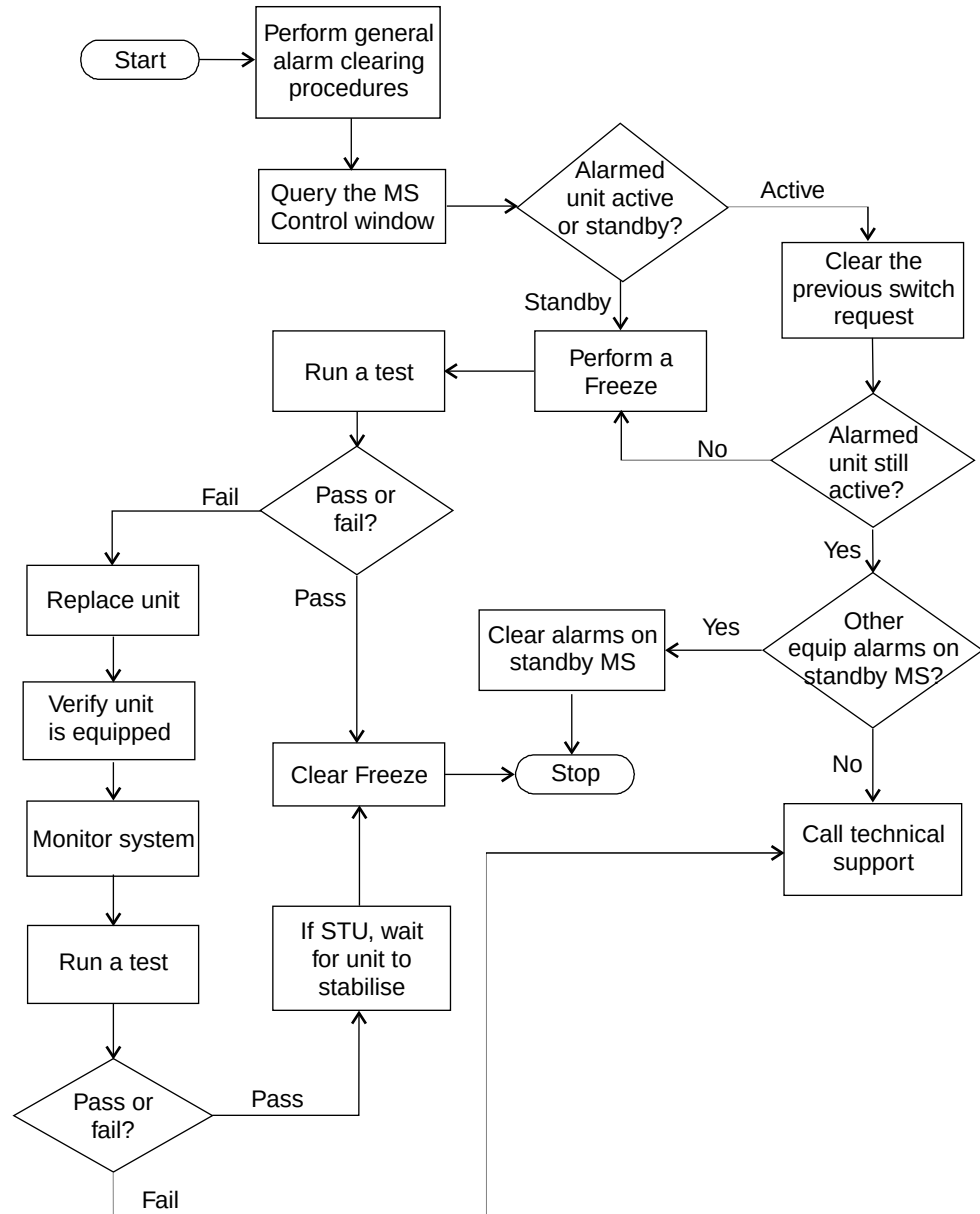
- 1 Call technical support before attempting to clear a Fault-cEQ (FLTcEQ) alarm on any equipment in the Main Controller (MC) subrack.

END OF STEPS



Flowchart for clearing a FLTcEQ on a BSC or STU

Flowchart The following flowchart shows the procedure for clearing a Fault-cEQ (FLTcEQ) alarm on a BSC or STU.



□

Clearing a FLTcEQ on a BSC or STU

Clearing actions Use this procedure to clear a Fault-cEQ (FLTcEQ) alarm on a BSC or STU:

- 1 Perform the “General alarm clearing procedure” (21-8).
- 2 Perform a query on the MS Control window at *Protection > Equipment > MS Control*. Record the Current Req value and the Unit Status for the alarmed unit.

- 3 Does the Unit Status column display Active or Standby?

If	Then
Active	Go to Step 4.
Standby	Go to Step 8.

- 4 Depending on the Current Req value, clear the previous switch request by performing a Clear Freeze, Clear Forced Switch, or Clear Manual Switch.

Reference:

Use the MS Control window at *Protection > Equipment > MS Control*.

- 5 Perform a query to verify that the alarmed unit switched to standby.

- 6 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 7.
No	Go to Step 8.

- 7 Are other equipment alarms present on the standby MS?

If	Then
Yes	Clear alarms on the standby MS.

If	Then
No	Quit this procedure and contact technical support.

- 8 Using the MS Control window, perform a Freeze.

- 9 Run a Unit diagnostic test on the alarmed unit.

Reference: For more information, see one of the following topics:

- “BSC Unit procedure” (12-68)
- “STU Unit procedure” (12-77)

- 10 Did the test pass or fail?

If	Then
The test passed	The alarm should clear. Go to Step 16.
The test failed	Go to Step 11.

- 11 Replace the defective unit.

Reference: For more information, see the following topics:

- “Removing a unit from the MS or port subrack” (2-11)
- “Inserting a unit into the MS or port subrack” (2-13)

- 12 Perform a query on the Unit window at *Provision > Equipment > Unit* to verify that the Unit Condition column for the unit now displays Unit provisioned and initialised.

- 13 Monitor the entire system for new alarms after replacing a BSC or STU. This will ensure that the system has returned to a stable condition, and that any alarms resulting from the loss of clocking have cleared. If an alarm does not clear, clear it with the alarm-clearing procedure for that alarm.

Result:

It may take up to 5 minutes for the alarms to clear.

- 14 Run a Unit diagnostic test on the new unit.

.....

15 Did the test pass or fail?

If	Then
The test passed	For an STU, wait for the unit to warm up and stabilise (5 to 15 minutes), then go to Step 16.
The test failed	Record the time and date this occurred, and call technical support.

.....

16 Perform a Clear Freeze.

.....

17 Return any defective units to technical support.

Reference:

For more information, see “Procedure for returning defective equipment” (22-5).

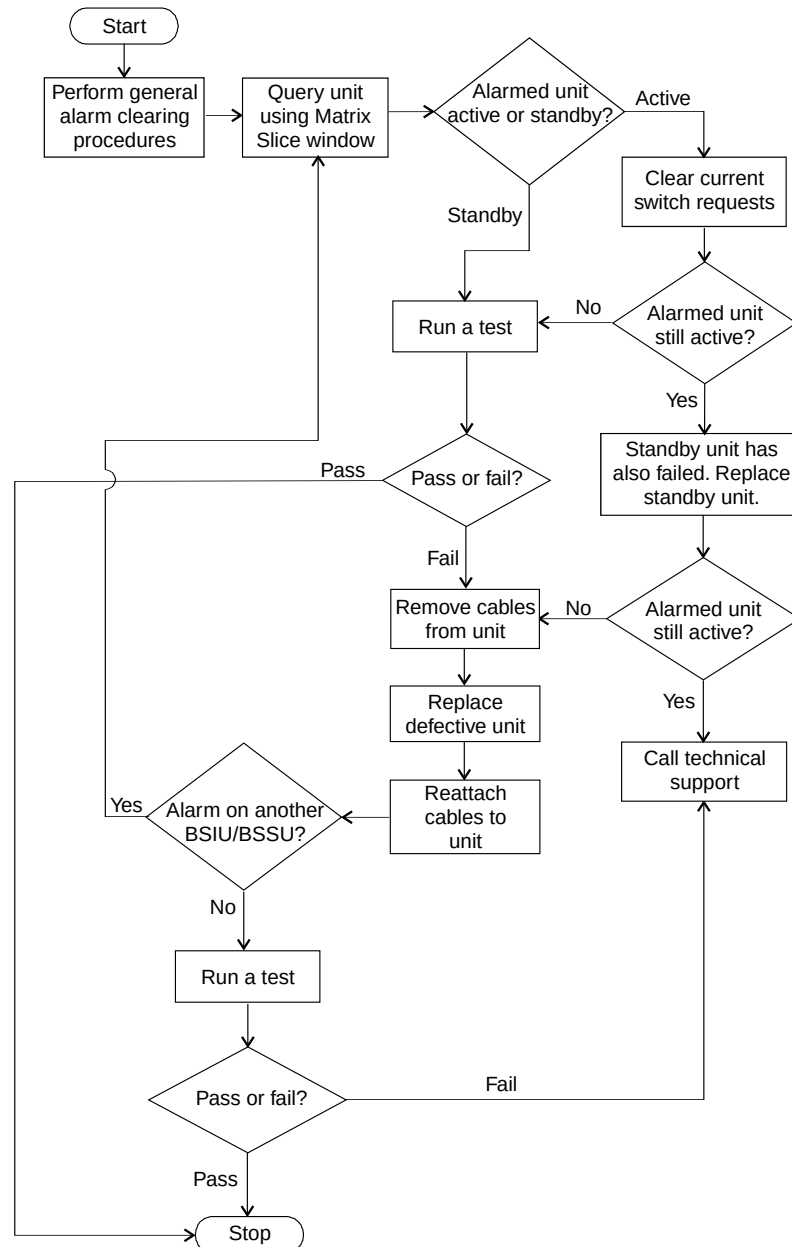
END OF STEPS

.....

☐

Flowchart for clearing a FLTcEQ on a BSIU or BSSU

Flowchart The following flowchart shows the procedure for clearing a Fault-cEQ (FLTcEQ) alarm on a BSIU or BSSU.



□

Clearing a FLTcEQ on a BSIU or BSSU

Clearing actions Use the following procedure to clear a Fault-cEQ (FLTcEQ) alarm on a BSIU or BSSU:

- 1 Perform the “General alarm clearing procedure” (21-8).
- 2 Query the alarmed unit using the Matrix Slice window at *Protection > Equipment > Matrix Slice*. Record the Current Req value and the Unit Status for the alarmed unit.

Reference:

Use the Matrix Slice window at *Protection > Equipment > Matrix Slice*.

- 3 Does the Unit Status column display Active or Standby?

If	Then
Active	Go to Step 4.
Standby	Go to Step 9.

- 4 Depending on the Current Req value, clear the previous switch request.

Reference:

Use the Matrix Slice window at *Protection > Equipment > Matrix Slice*.

- 5 Perform another query to verify that the alarmed unit switched to standby.

- 6 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 9.
No	The standby unit has also failed. Replace the standby unit and continue to Step 7.

- 7 Perform another query to verify that the alarmed unit switched to standby.

8 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 9.
No	Quit this procedure and contact technical support.

9 Run a BSIU or BSSU Unit diagnostic test on the alarmed unit.

Reference:

For more information, see “BSIU and BSSU Unit procedure” (12-71).

10 Did the test pass or fail?

If	Then
The test passed	The alarm should clear. Quit this procedure.
The test failed	Go to Step 11.

11 Remove the cables from the unit.

Reference: For more information, see the following topics:

- “Inserting a cable” (3-3)
- “Removing a cable” (3-4)

12 Replace the defective unit.

Reference: For more information, see the following topics:

- “Removing a unit from the MS or port subrack” (2-11)
- “Inserting a unit into the MS or port subrack” (2-13)

13 Reattach the cables to the unit.

14 Run a BSIU or BSSU Unit diagnostic test on the new unit.

15 Did the test pass or fail?

If	Then
The test passed	Go to Step 16.
The test failed	Record the time and date this occurred, and call technical support.

-
- 16** If there is a FLTcEQ alarm on another BSIU or BSSU, return to Step 2.
-

- 17** Return any defective units to technical support.

Reference:

For more information, see “Procedure for returning defective equipment” (22-5).

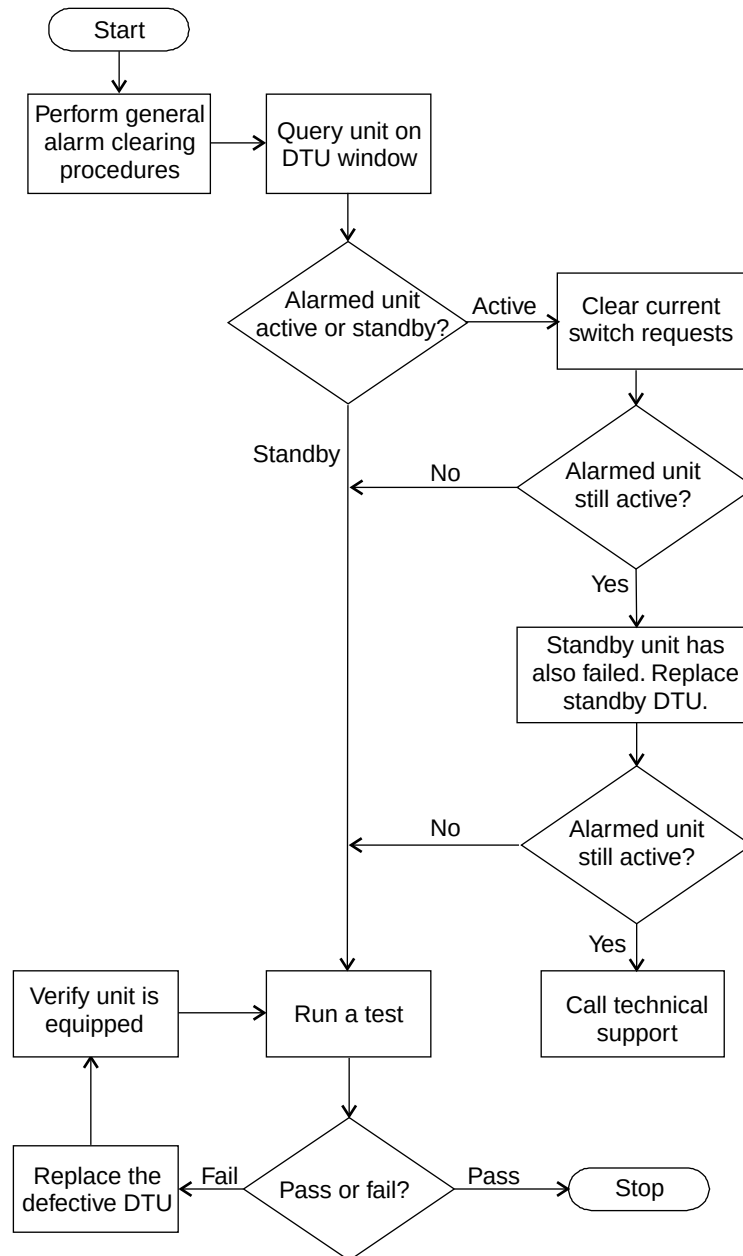
END OF STEPS

.....



Flowchart for clearing a FLTcEQ on a DTU

Flowchart The following flowchart shows the procedure for clearing a Fault-cEQ (FLTcEQ) alarm on a DTU.



□

Clearing a FLTcEQ on a DTU

Clearing actions Use the following procedure to clear a Fault-cEQ (FLTcEQ) alarm on a DTU:

- 1 Perform the “General alarm clearing procedure” (21-8).
- 2 Query the alarmed unit using the DTU window at *Protection > Equipment > DTU*. Record the Current Req value and Unit Status for the alarmed unit.

- 3 Does the Unit Status column display Active or Standby?

If	Then
Active	Go to Step 4.
Standby	Go to Step 9.

- 4 Depending on the Current Req value, clear the previous switch request by performing a Clear Freeze, Clear Forced Switch, or Clear Manual Switch.

Reference:

Use the DTU window at *Protection > Equipment > DTU*.

- 5 Perform another query to verify that the alarmed unit switched to standby.

- 6 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 9.
No	The standby unit has also failed. Replace the standby unit and continue to Step 7.

- 7 Perform another query to verify that the alarmed unit switched to standby.

- 8 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 9.
No	Quit this procedure and contact technical support.

- 9 Run a DTU Unit diagnostic test on the alarmed unit.

Reference:

For more information, see “DTU Unit procedure” (12-74).

- 10 Did the test pass or fail?

If	Then
The test passed	The alarm should clear. Quit this procedure.
The test failed	Go to Step 11.

- 11 Replace the defective unit.

Reference: For more information, see the following topics:

- “Removing a unit from the MS or port subrack” (2-11)
- “Inserting a unit into the MS or port subrack” (2-13)

- 12 Run a DTU Unit diagnostic test on the new unit.

- 13 Did the test pass or fail?

If	Then
The test passed	Go to Step 14.
The test failed	Record the time and date this occurred, and call technical support.

- 14 Return any defective units to technical support.

Reference:

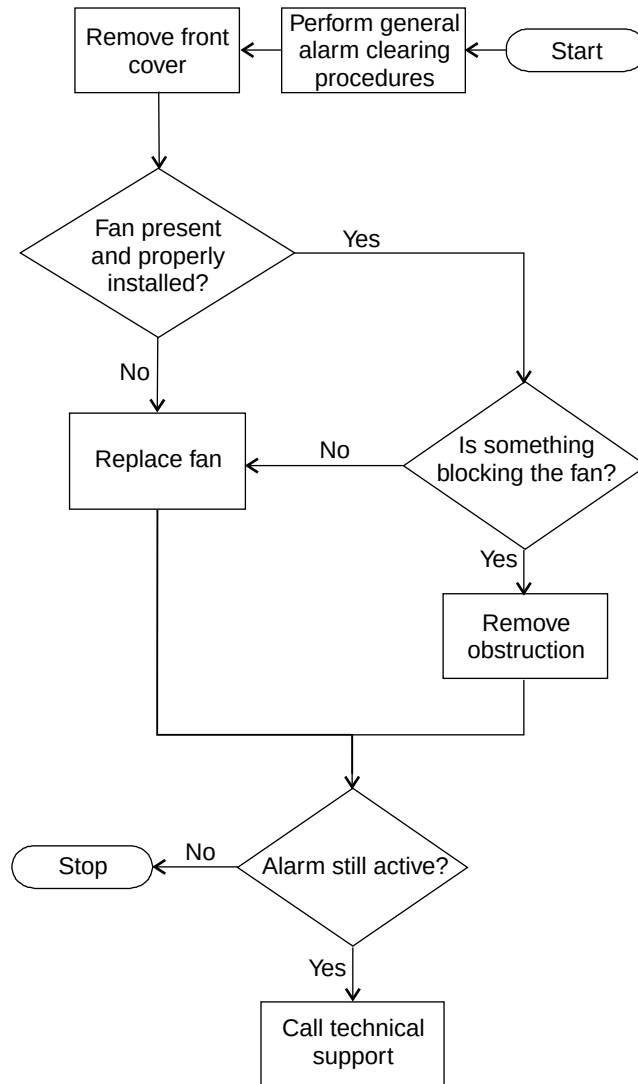
For more information, see “Procedure for returning defective equipment” (22-5).

END OF STEPS



Flowchart for clearing a FLTcEQ on a fan in the MC subrack

Flowchart The following flowchart shows the procedure for clearing a Fault-cEQ (FLTcEQ) alarm on a fan in the MC subrack.

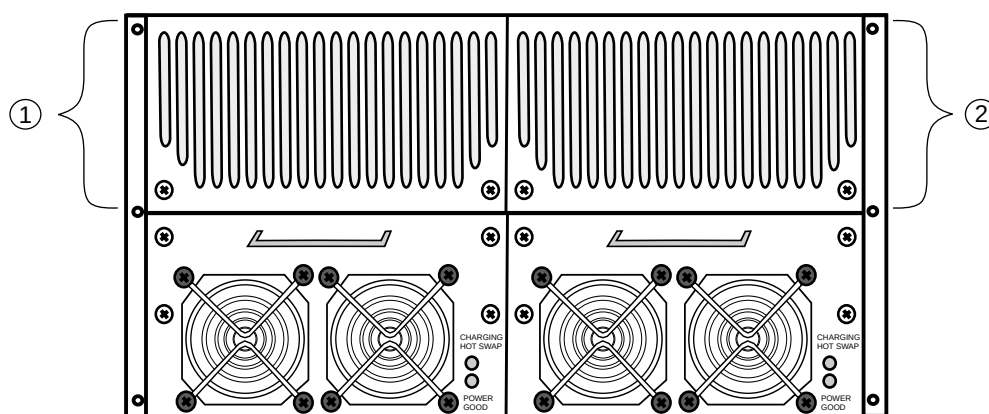


□

Clearing a FLTcEQ on a fan in the MC subrack

About the fans Four DC-powered fans provide forced air cooling for the Main Controller (MC) subrack. The fans are mounted in two trays below the units. Each tray contains two fans. If you need to replace a fan, replace the entire fan tray containing the defective fan as a single assembly. You can replace the tray without having to remove power from the system.

The following graphic is a front view showing the two fan trays.



Legend:

1. First fan tray
2. Second fan tray (for duplicated MC configuration)

Possible causes of a FLTcEQ fan alarm

The system will generate a Fault-cEQ (FLTcEQ) fan alarm for any of the following reasons:

- The fan is not physically present and correctly installed
- Something is blocking the free flow of air through the fan
- The fan is defective

Clearing actions

Use the following procedure to clear a FLTcEQ alarm on a fan in the MC subrack:

- 1 Perform the “General alarm clearing procedure” (21-8).
- 2 Remove the front cover of the Main Controller subrack, if present.
- 3 Is the fan physically present and properly installed?

If	Then
Yes	Go to Step 4.
No	Go to Step 7.

- 4 Is something blocking the free flow of air through the fan?

If	Then
Yes	Go to Step 5.
No	Go to Step 7.

- 5 Remove any obstructions that are restricting free air flow through the fan.

- 6 Is the alarm still present?

If	Then
Yes	Go to Step 7.
No	Quit this procedure.

- 7 Remove the fan by loosening the two quarter-turn fasteners that are located on the front of the fan tray in the lower left and right corners.

- 8 Slide the fan tray out of the rack.

Important! If you do not have a duplicated Main Controller configuration, you can swap the defective fan with the fan located on the other side of the Main Controller subrack.

- 9 Slide the new fan tray into the rack. Use firm steady pressure to seat the connectors properly.

- 10 Tighten the two quarter-turn fasteners that hold the tray in the rack.

- 11 Replace the cover.

- 12 Return any defective fans to technical support.

Reference:

For more information, see “Procedure for returning defective equipment” (22-5).

E N D O F S T E P S



Clearing a FLTcEQ on an IU or an unprotected port unit

Purpose Use this procedure to clear a Fault-cEQ (FLTcEQ) alarm on an IU, or an unprotected port unit. An STM-1 unit is unprotected if neither 1:8 equipment protection nor MSP is assigned.

Avoiding service interruptions for STM-1 electrical

The following procedure will cause a service interruption. If the alarmed unit is an STM-1 electrical unit, you can insert a protection unit into slot 9 or 19.

Related topic

To avoid a service interruption, perform the procedure in “Clearing a FLTcEQ on an STM-1 electrical unit that uses 1:8 equipment protection” (21-77).

Clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
-

- 2 For an alarm on a port unit, run the appropriate Unit diagnostic test on the alarmed unit.

Reference:

For more information, see “All other equipment diagnostic tests” (12-81).

- 3 Did the test pass or fail?

If	Then
The test passed	The alarm should clear. Quit this procedure.
The test failed	Go to Step 4.

- 4 For an IU, remove the cables from the unit.

Reference: For more information, see the following topics:

- “Inserting a cable” (3-3)
- “Removing a cable” (3-4)



CAUTION

Removing a unit that is carrying service will cause a disruption of service.

- 5 Replace the defective unit.

Reference: For more information, see the following topics:

- “Removing a unit from the MS or port subrack” (2-11)
- “Inserting a unit into the MS or port subrack” (2-13)

- 6 For an IU, reattach the cables to the unit.

- 7 For an alarm on a port unit, run the appropriate Unit diagnostic test on the new unit.

- 8 Did the test pass or fail?

If	Then
The test passed	Go to Step 9.
The test failed	Record the time and date this occurred, and call technical support.

- 9 Return any defective units to technical support.

Reference:

For more information, see “Procedure for returning defective equipment” (22-5).

END OF STEPS



Clearing a FLTcEQ on an MPU

Clearing actions

- 1 Use the procedure to remove an MPU to clear a Fault-cEQ (FLTcEQ) alarm.

Reference: For more information, see one of the following:

- “Removing the MPU on a single MC configuration” (11-22)
- “Removing the MPU on a duplicated MC configuration” (11-18)

END OF STEPS



Clearing a FLTcEQ on an MSU

Clearing actions

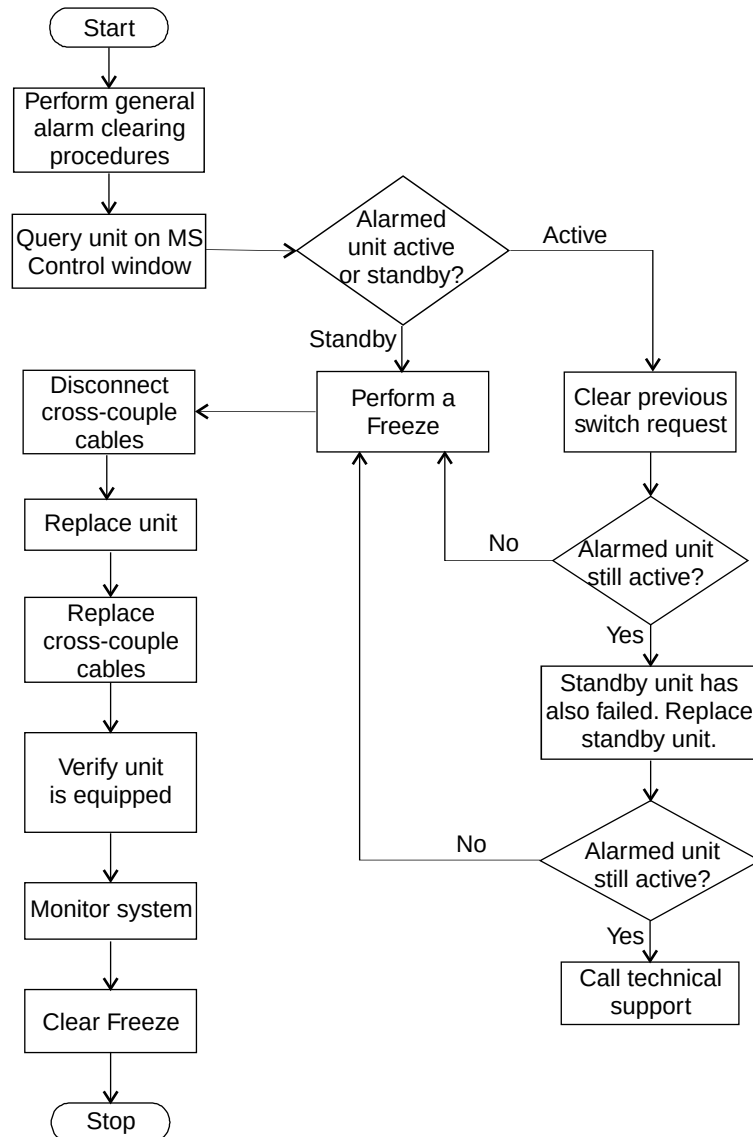
- 1 Call technical support before attempting to clear a Fault-cEQ (FLTcEQ) alarm on any equipment in the Main Controller (MC) subrack.

END OF STEPS



Flowchart for clearing a FLTcEQ on an OLU

Flowchart The following flowchart shows the procedure for clearing a Fault-cEQ (FLTcEQ) alarm on an OLU.



Clearing a FLTcEQ on an OLU

Clearing actions Use the following procedure to clear a Fault-cEQ (FLTcEQ) alarm on an OLU:

- 1 Perform the “General alarm clearing procedure” (21-8).

- 2 Perform a query on the MS Control window at *Protection > Equipment > MS Control*. Record the Current Req value and the Unit Status for the alarmed unit.

- 3 Does the Unit Status column display Active or Standby?

If	Then
Active	Go to Step 4.
Standby	Go to Step 9.

- 4 Depending on the Current Req value, clear the previous switch request.

Reference:

Use the MS Control window at *Protection > Equipment > MS Control*.

- 5 Perform a query to verify that the alarmed unit switched to standby.

- 6 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 9.
No	The standby unit has also failed. Replace the standby unit and continue to Step 7.

- 7 Perform a query to verify that the alarmed unit switched to standby.

- 8 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 9.
No	Quit this procedure and contact technical support.

.....

9 Using the MS Control window, perform a Freeze.

.....

10 Disconnect the cross-couple cables.

.....

11 Replace the defective unit.

Reference: For more information, see the following topics:

- “Removing a unit from the MS or port subrack” (2-11)
 - “Inserting a unit into the MS or port subrack” (2-13)
-

12 Reconnect the cross-couple cables.

.....

13 Perform a query on the Unit window at *Provision > Equipment > Unit* to verify that the Unit Condition column for the unit now displays Unit provisioned and initialised.

.....

14 Monitor the entire system for new alarms after replacing an OLU. This will ensure that the system has returned to a stable condition, and that any alarms resulting from the loss of clocking have cleared. If an alarm does not clear, clear it with the alarm-clearing procedure for that alarm.

Result:

It may take up to 5 minutes for the alarms to clear.

.....

15 Perform a Clear Freeze.

.....

16 Return any defective units to technical support.

Reference:

For more information, see “Procedure for returning defective equipment” (22-5).

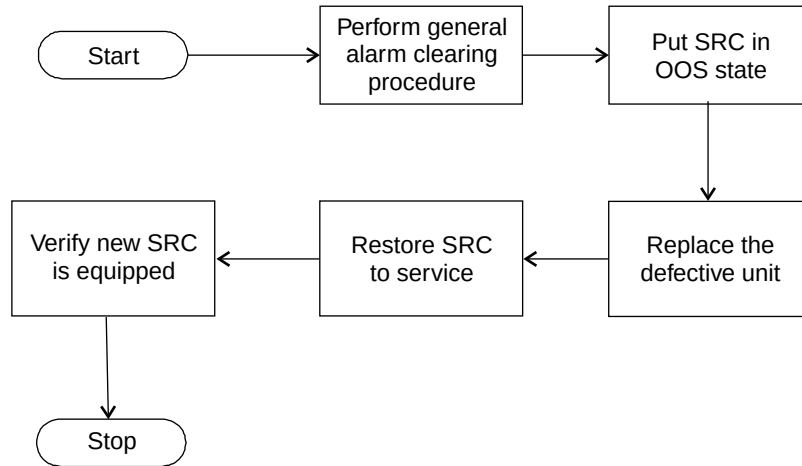
END OF STEPS

.....



Flowchart for clearing a FLTcEQ on an SRC

Flowchart The following flowchart shows the procedure for clearing a Fault-cEQ (FLTcEQ) alarm on an SRC unit.



Clearing a FLTcEQ on an SRC

Clearing actions Use the following procedure to clear a Fault-cEQ (FLTcEQ) alarm on an SRC:

- 1 Perform the “General alarm clearing procedure” (21-8).
-

- 2 Put the SRC in the out-of-service state.

Reference: For more information, see one of the following topics:

- “Removing an MS subrack SRC from service” (11-33)
 - “Removing a port subrack SRC from service” (11-34)
-

- 3 Replace the defective unit.

Reference: For more information, see the following topics:

- “Removing a unit from the MS or port subrack” (2-11)
 - “Inserting a unit into the MS or port subrack” (2-13)
-

- 4 Restore the SRC to service.

Reference:

For more information, see “Restoring an SRC to service” (11-35).

- 5 Query the SRC unit using the Unit window at *Provision > Equipment > Unit* to make sure it booted gracefully.

Result:

The SRC should display `Unit provisioned and initialised`.

- 6 Return any defective units to technical support.

Reference:

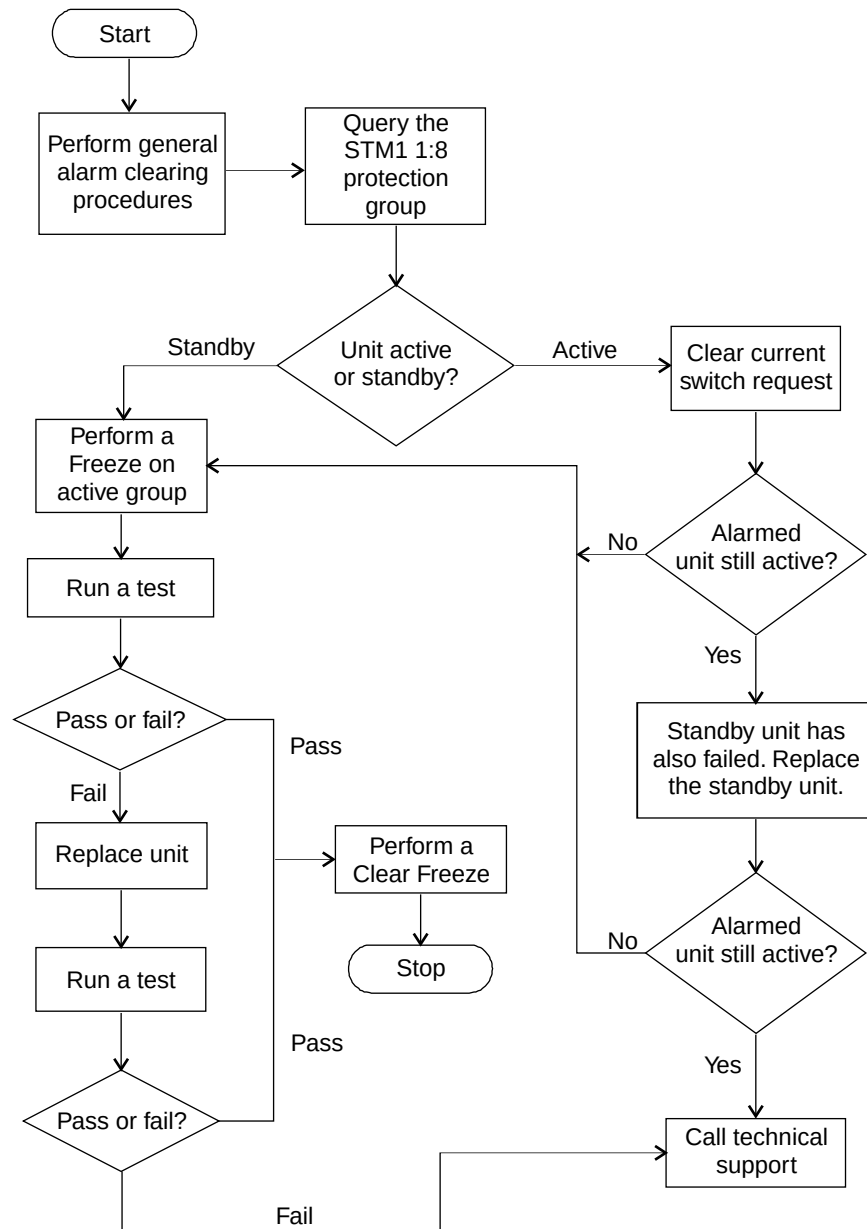
For more information, see “Procedure for returning defective equipment” (22-5).

END OF STEPS



Flowchart for clearing a FLTcEQ on an STM-1 electrical unit that uses 1:8 equipment protection

Flowchart The following flowchart shows the procedure for clearing a Fault-cEQ (FLTcEQ) alarm on an STM-1 electrical unit that uses 1:8 equipment protection.



□

Clearing a FLTcEQ on an STM-1 electrical unit that uses 1:8 equipment protection

Clearing actions Use the following procedure to clear a Fault-cEQ (FLTcEQ) alarm on an STM-1 electrical unit that uses 1:8 equipment protection:

- 1 Perform the “General alarm clearing procedure” (21-8).
- 2 Query the STM-1 1:8 protection group using the STM1 1:8 window at *Protection > Equipment > STM1 1:8*. Record the Current Req value and the Unit Status for the alarmed unit.

- 3 Does the Unit Status column display Active or Standby?

If	Then
Active	Go to Step 4.
Standby	Go to Step 9.

- 4 Depending on the Current Req value, clear the previous switch request.

Reference:

Use the STM1 1:8 window at *Protection > Equipment > STM1 1:8*.

- 5 Perform another query to verify that the alarmed unit switched to standby.

- 6 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 9.
No	The standby unit has also failed. Replace the standby unit and continue to Step 7.

- 7 Perform another query to verify that the alarmed unit switched to standby.

Clearing a FLTcEQ on an STM-1 electrical unit that uses 1:8 equipment protection

8 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 9.
No	Quit this procedure and contact technical support.

9 For the active unit, perform a Freeze.

10 Run an STM-1 Unit diagnostic test on the alarmed unit.

Reference:

For more information, see “All other equipment diagnostic tests” (12-81).

11 Did the test pass or fail?

If	Then
The test passed	The alarm should clear. Go to Step 15.
The test failed	Go to Step 12.

12 Replace the unit.

Reference: For more information, see the following topics:

- “Removing a unit from the MS or port subrack” (2-11)
- “Inserting a unit into the MS or port subrack” (2-13)

13 Run an STM-1 Unit diagnostic test on the new unit.

14 Did the test pass or fail?

If	Then
The test passed	Go to Step 15.
The test failed	Record the time and date this occurred, and call technical support.

15 Perform a Clear Freeze.

Clearing a FLTcEQ on an STM-1 electrical
unit that uses 1:8 equipment protection

-
- 16** Return any defective units to technical support.

Reference:

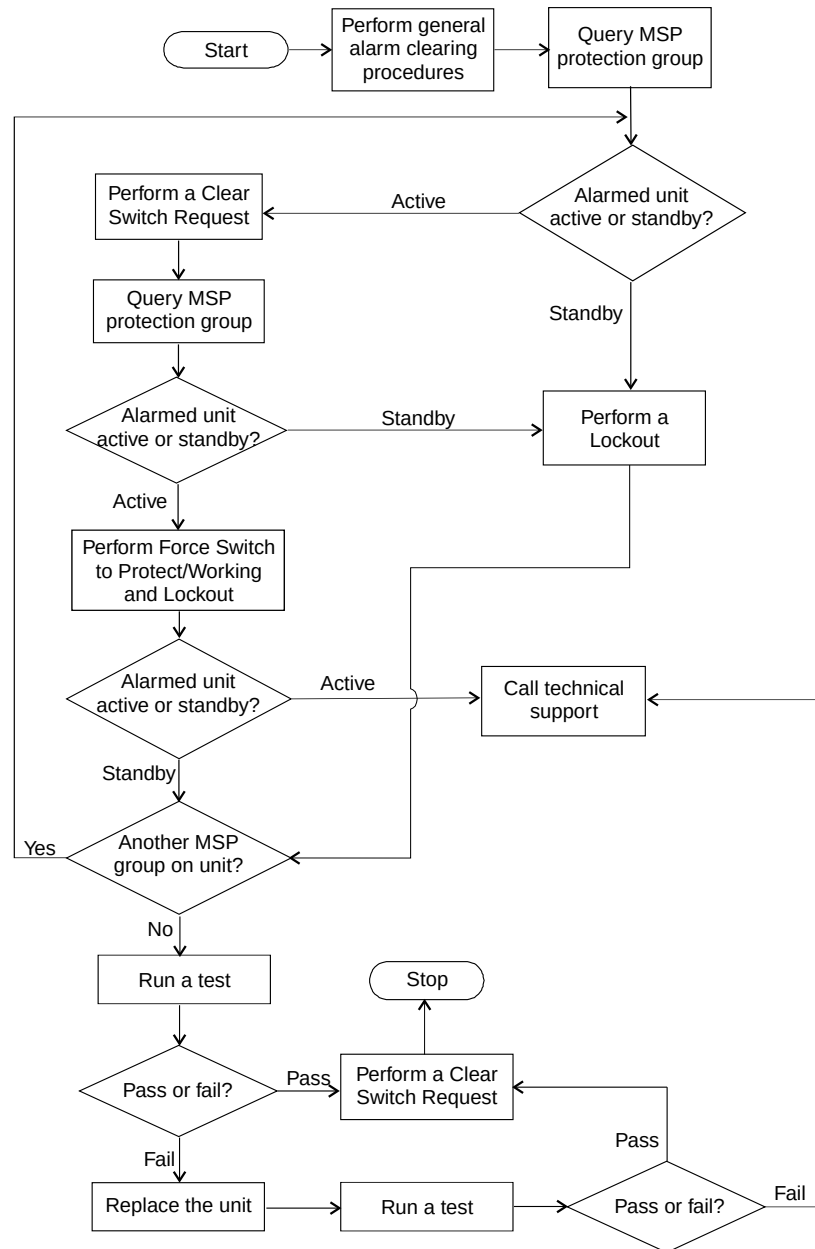
For more information, see “Procedure for returning defective
equipment” (22-5).

END OF STEPS



Flowchart for clearing a FLTcEQ on a port unit that uses NTT MSP

Flowchart The following flowchart shows the procedure for clearing a Fault-cEQ (FLTcEQ) alarm on a protection or working port unit that uses NTT MSP.



Clearing a FLTcEQ on a port unit that uses NTT MSP

Clearing actions Use the following procedure to clear a Fault-cEQ (FLTcEQ) alarm on a working or protection port unit that uses NTT MSP:

- 1 Perform the “General alarm clearing procedure” (21-8).

- 2 Do the following steps for *every* MSP group on the alarmed unit.

- 3 Query the MSP protection group.

Reference:

Use the MSP window at *Protection Switch > Transmission > MSP*.

- 4 Does the Unit Status column for the alarmed unit display Active or Standby?

If	Then
Active	Go to Step 5.
Standby	Go to Step 12.

- 5 Perform a Clear Switch Request.

Reference:

Use the MSP window at *Protection Switch > Transmission > MSP*.

- 6 Query the MSP protection group again.

- 7 Is the alarmed unit active or standby?

If	Then
Active	Go to Step 8.
Standby	Go to Step 12.

- 8 Is the alarmed unit working or protection?

If	Then
Working	Perform a Forced Switch to Protect.
Protection	Perform a Forced Switch to Working.

- 9 Perform a Lockout request.

Reference:

Use the MSP window at *Protection Switch > Transmission > MSP*.

- 10 Perform another query to verify that the alarmed unit switched to standby.

- 11 Is the alarmed unit active or standby?

If	Then
Active	Quit this procedure and contact technical support.
Standby	Go to Step 13.

- 12 Perform a Lockout request.

- 13 Is there another MSP group on the unit?

If	Then
Yes	Return to Step 3.
No	Go to Step 14.

- 14 Run a Unit diagnostic test on the alarmed unit.

Reference:

For more information, see “All other equipment diagnostic tests” (12-81).

- 15 Did the test pass or fail?

If	Then
The test passed	The alarm should clear. Go to Step 19.

Clearing a FLTcEQ on a port unit that uses
NTT MSP

If	Then
The test failed	Go to Step 16.

.....

16 Replace the unit.

Reference: For more information, see the following topics:

- “Removing a unit from the MS or port subrack” (2-11)
 - “Inserting a unit into the MS or port subrack” (2-13)
-

17 Run a Unit diagnostic test on the new unit.

.....

18 Did the test pass or fail?

If	Then
The test passed	Go to Step 19.
The test failed	Record the time and date this occurred, and call technical support.

.....

19 Perform *two* Clear Switch Requests.

.....

20 Return any defective units to technical support.

Reference:

For more information, see “Procedure for returning defective equipment” (22-5).

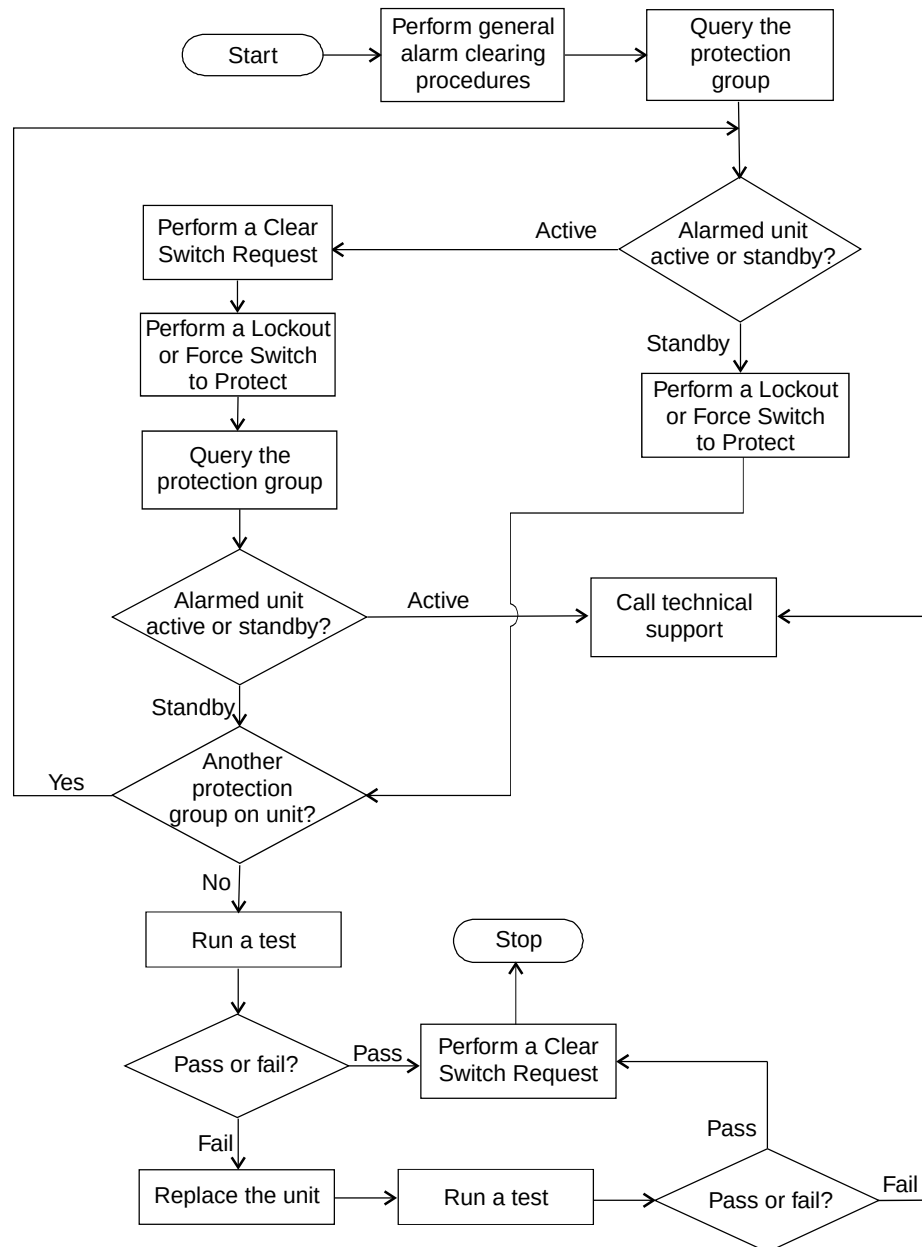
END OF STEPS

.....



Flowchart for clearing a FLTcEQ on a port unit that uses SNCP, ITU MSP, or ANSI MSP

Flowchart The following flowchart shows the procedure for clearing a Fault-cEQ (FLTcEQ) alarm on a working or protection port unit that uses SNCP, ITU MSP, or ANSI MSP.



Clearing a FLTcEQ on a port unit that uses SNCP, ITU MSP, or ANSI MSP

Clearing actions Use the following procedure to clear a Fault-cEQ (FLTcEQ) alarm on a working or protection port unit that uses SNCP, ITU MSP, or ANSI MSP:

- 1 Perform the “General alarm clearing procedure” (21-8).
- 2 Do the following steps for *every* protection group on the alarmed unit.
- 3 Query the protection group.

Reference: Use one of the following windows:

- *Protection Switch > Transmission > MSP*
- *Protection Switch > Transmission > SNCP*

- 4 Does the Unit Status column display Active or Standby?

If	Then
Active	Go to Step 5.
Standby	Go to Step 9.

- 5 Perform a Clear Switch Request.

Reference: Use one of the following windows:

- *Protection Switch > Transmission > MSP*
- *Protection Switch > Transmission > SNCP*

- 6 Is the alarmed unit working or protection?

If	Then
Working	Perform a Forced Switch to Protect.
Protection	Perform a Lockout request.

- 7 Query the protection group again.

- 8 Is the protection port active or standby?

Clearing a FLTcEQ on a port unit that uses
SNCP, ITU MSP, or ANSI MSP

If	Then
Active	Quit this procedure and call technical support.
Standby	Go to Step 10.

9 Is the alarmed unit working or protection?

If	Then
Working	Perform a Forced Switch to Protect.
Protection	Perform a Lockout request.

10 Is there another protection group on the unit?

If	Then
Yes	Return to Step 3.
No	Go to Step 11.

11 Run a Unit diagnostic test on the alarmed unit.

Reference:

For more information, see “All other equipment diagnostic tests” (12-81).

12 Did the test pass or fail?

If	Then
The test passed	The alarm should clear. Go to Step 16.
The test failed	Go to Step 13.

13 Replace the unit.

Reference: For more information, see the following topics:

- “Removing a unit from the MS or port subrack” (2-11)
- “Inserting a unit into the MS or port subrack” (2-13)

14 Run a Unit diagnostic test on the new unit.

15 Did the test pass or fail?

Clearing a FLTcEQ on a port unit that uses
SNCP, ITU MSP, or ANSI MSP

If	Then
The test passed	Go to Step 16.
The test failed	Record the time and date this occurred, and call technical support.

.....

16 Perform a Clear Switch Request.

.....

17 Return any defective units to technical support.

Reference:

For more information, see “Procedure for returning defective equipment” (22-5).

.....

END OF STEPS

.....



FLTcSW

Overview

Purpose This section contains information about FLTcSW alarms.

Organisation This section contains the following information:

- “FLTcSW description” (21-89)
- “Clearing FLTcSW alarms on the MPU” (21-91)
- “Clearing FLTcSW alarms on the SRC” (21-92)



FLTcSW description

Definition An FLTcSW alarm indicates a safepoint failure caused by a software communication failure on the MPU, or a software failure on the SRC. This alarm can also indicate that the system software has reached an inconsistent state because the cable between the DUP connectors on the Matrix and Synchronisation subrack connector panel is loose or not connected.

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The yellow LED on the affected MPU or the red LED on the affected SRC is continuously lit.



Clearing FLTcSW alarms for DUP cable problems

Clearing action



CAUTION

Do not attempt to replace or reattach the DUP cable without technical assistance. In certain cases, replacing or reattaching the DUP cable may cause a loss of service.

- 1** If the cable between the DUP connectors on the Matrix and Synchronisation subrack connector panel is loose, missing, or broken, call technical support for assistance.

END OF STEPS



Clearing FLTcSW alarms on the MPU

Clearing actions



CAUTION

Do not remove any units without following the appropriate procedures. You could accidentally cause a service interruption, corrupt the hard disk, or power down a subrack and then have to reload the software from the Magneto Optical (MO) disks.

Important! Call technical support before attempting to clear a FLTcSW alarm on the MPU.

- 1 Perform the “General alarm clearing procedure” (21-8).
-



CAUTION

You will lose the user interface after performing the following step.

- 2 Put the MPU in the out-of-service state.

Reference:

For more information, see “Removing the MPU on a duplicated MC configuration” (11-18).

- 3 Restore the MPU to service.

Reference: For more information, see one of the following:

- “Restoring the DB on an MPU with a duplicated MC configuration” (11-23)
- “Restoring the DB on an MPU with a single MC configuration” (11-29)

END OF STEPS



Clearing FLTcSW alarms on the SRC

Clearing actions



CAUTION

Do not remove any units without following the appropriate procedures. You could accidentally cause a service interruption, corrupt the hard disk, or power down a subrack and then have to reload the software from the Magneto Optical (MO) disks.

- 1 Perform the “General alarm clearing procedure” (21-8).
 - 2 Verify that the LAN cable to the SRC is correct.
 - 3 If the alarm does not clear, put the SRC in the out-of-service state.
-

Reference: For more information, see one of the following topics:

- “Removing an MS subrack SRC from service” (11-33)
 - “Removing a port subrack SRC from service” (11-34)
-

- 4 Restore the SRC to service.

Reference:

For more information, see “Restoring an SRC to service” (11-35).

- 5 If the alarm still does not clear, replace the SRC.

Reference:

For more information, see “Clearing a FLTcEQ on an SRC” (21-75).

END OF STEPS



HPcDEG

Overview

Purpose This section contains information about HPcDEG alarms.

Organisation This section contains the following information:

- “HPcDEG description” (21-94)
- “Clearing HPcDEG alarms” (21-95)



HPcDEG description

Definition	An HPcDEG alarm indicates a Higher order Path Degraded Bit Error Rate. The equivalent bit error rate of the incoming signal exceeds the provisioned signal degrade threshold.
Alarm type	Transmission
Default severity level	You can change the severity levels. The default severity levels are as follows: • Prompt for failures that affect service • Information for failures that do not affect service
Local results	For Prompt alarms, a Prompt alarm indicator lights on the following: • User Panel • End-of-suite • Rack-top • Station For Information alarms, an Information alarm indicator on the User Panel lights. For Prompt and Information alarms, the red LED on the affected port unit flashes.



Clearing HPcDEG alarms

Alarm clearing action Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:

- A description of the problem
- A request asking the administrator to examine the relevant upstream equipment



HPcPLM

Overview

Purpose This section contains information about HPcPLM alarms.

Organisation This section contains the following information:

- “HPcPLM description” (21-97)
- “Clearing HPcPLM alarms” (21-98)



HPcPLM description

Definition An HPcPLM alarm indicates a Higher order Path Payload Label Mismatch. The received path signal label value that is used to indicate the composition of the VC-3, VC-4, or VC4-4c payload does not match the expected value. The expected value may be equipped nonspecific, VC-4 TUG structured, or unequipped if provisioned as supervised unequipped.

Alarm type Transmission

Default severity level You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected port unit flashes.

Remote results The system does the following in the remote directions:

- Generates an HPaRDI notification in the upstream direction
- Inserts Alarm Indication Signal (AIS) into the transmission signal in the downstream direction



Clearing HPcPLM alarms

Alarm clearing action Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:

- A description of the problem
- A request asking the administrator to examine the relevant upstream equipment



HPcRDI

Overview

Purpose This section contains information about HPcRDI alarms.

Organisation This section contains the following information:

- “HPcRDI description” (21-100)
- “Clearing HPcRDI alarms” (21-101)



HPcRDI description

Definition	An HPcRDI alarm indicates a Higher order Path Remote Defect Indicator. The system has received an RDI indication. The downstream equipment has detected transmission that was interrupted at its receive side and is returning RDI.
Alarm type	Transmission
Default severity level	You can change the severity levels. The default severity levels are as follows: • Prompt for failures that affect service • Information for failures that do not affect service
Local results	For Prompt alarms, a Prompt alarm indicator lights on the following: • User Panel • End-of-suite • Rack-top • Station For Information alarms, an Information alarm indicator on the User Panel lights. For Prompt and Information alarms, the red LED on the affected port unit flashes.



Clearing HPcRDI alarms

Alarm clearing actions

- 1 Clear all relevant equipment and transmission alarms that may be active on your own system.

- 2 If HPcRDI persists, check the local equipment that is connected to the downstream equipment.

END OF STEPS



HPcTIM

Overview

Purpose This section contains information about HPcTIM alarms.

Organisation This section contains the following information:

- “HPcTIM description” (21-103)
- “Clearing HPcTIM alarms” (21-104)



HPcTIM description

Definition An HPcTIM alarm indicates a Higher order Path Trace Identifier Mismatch. The received path trace identifier that is used to verify the continued connection to the intended transmitter does not match the provisioned value.

Incorrect routing exists somewhere in this system or in the upstream direction because:

- Line cables are connected incorrectly or the wrong cross-connections were made upstream
- The Network Element that reported the alarm has the wrong expected Path Trace Identifier (PTI)
- The far-end Network Element has the wrong transmitted PTI

Alarm type Transmission

Default severity level You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected port unit flashes.

Remote results The system does the following in the remote directions:

- Generates an HPaRDI notification in the upstream direction
- Inserts Alarm Indication Signal (AIS) into the transmission signal in the downstream direction



Clearing HPcTIM alarms

Alarm clearing action Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:

- A description of the problem
- A request asking the administrator to examine the relevant upstream equipment



HPcUNEQ

Overview

Purpose This section contains information about HPcUNEQ alarms.

Organisation This section contains the following information:

- “HPcUNEQ description” (21-106)
- “Clearing HPcUNEQ alarms” (21-107)



HPcUNEQ description

Definition	Higher order Path Unequipped. An HPcUNEQ alarm is activated when the system receives an unequipped signal label. This happens when an intermediate system is provisioned incorrectly and is not transmitting the intended signal.
Alarm type	Transmission
Default severity level	You can change the severity levels. The default severity levels are as follows: • Prompt for failures that affect service • Deferred for failures that do not affect service
Local results	A Prompt or Deferred alarm indicator lights on the following: • User Panel • End-of-suite • Rack-top • Station The red LED on the affected port unit flashes.



Clearing HPcUNEQ alarms

- Alarm clearing action** Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:
- A description of the problem
 - A request asking the administrator to examine the relevant upstream equipment



INTFcEQ

Overview

Purpose This section contains information about INTFcEQ alarms.

Organisation This section contains the following information:

- “INTFcEQ description” (21-109)
- “INTFcEQ interfaces and addresses” (21-110)
- “Clearing INTFcEQ alarms” (21-111)



INTFcEQ description

Definition An INTFcEQ alarm indicates an interface failure in an internal communication link.

This alarm is applicable to the following interfaces:

- Bit Slice Fibre Interface (BSFI) — OLU to BSSU
- Equipment Core Interface (ECI) — BSSU to BSIU
- Equipment Physical Interface (EPI) — BSIU to port unit
- Port Subrack Control Interface (PCI) — BSIU to DTU, STU to BSC, DTU to port unit
- Cross-couple link between the working DTU and the protection DTU in a port subrack

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station



INTFcEQ interfaces and addresses

INTFcEQ interfaces AN INTFcEQ alarm usually means that there is an interface failure in an internal communication link affecting one of the following interfaces:

- OLU and BSSU
- BSSU and BSIU
- DTU and port unit
- DTU and BSIU
- BSC and STU
- BSIU and port unit

How INTFcEQ addresses are displayed The following table displays the interfaces that are reported with an INTFcEQ alarm.

Interface	Unit alarmed	Alarm displayed on...
BSFI	OLU or BSSU	MS-3-OLU-{1–4}-BSFI{1–5}
ECI	BSSU or BSIU	MS-3-BSSU-{1–10}-ECI{1–8}
ECI	BSSU or BSIU	PSA-{4–19}-BSIU-{1–10}-ECI{1, 2}
ECI	BSSU or BSIU	PSC-{4–19}-BSIU-{1–10}-ECI{1–4}
PCI	STM-(N) or BSIU	{PSA, PSC}-{4–19}-BSIU-{1–10}-DTU{1, 2}
PCI	STU	MS-3-STU-{1, 2}-PCI-BSC
EPI	STM-(N)	{PSA, PSC}-{4–19}-{STM1, STM4, STM16}-{1–9, 11–18}-BSIU{1–10}

Related topic For more information, see “Example of a fibre address” (5-19). □

Clearing INTFcEQ alarms

Clearing actions

- 1 Replace the unit reporting the alarm by using the appropriate Fault-cEQ (FLTcEQ) procedure.

Example:

If the alarm is reported on the DTU, use the procedure for clearing a FLTcEQ on a DTU.

Reference:

To locate the appropriate FLTcEQ unit-replacement procedure, see “FLTcEQ flowcharts and procedures” (21-48).

- 2 If the alarm does not clear, use the appropriate FLTcEQ procedure for the second unit.
-

- 3 If the alarm does not clear, call technical support.

END OF STEPS



INVcCONF

Overview

Purpose This section contains information about INVcCONF alarms.

Organisation This section contains the following information:

- “INVcCONF description” (21-113)
- “Clearing INVcCONF alarms” (21-114)



INVcCONF description

Definition An INVcCONF alarm indicates an Invalid Configuration. A unit has been inserted into a slot that is not valid for that subrack type and configuration.

The INVcCONF alarm is activated against the SRC for the appropriate port subrack.

Alarm type Equipment

Default severity level You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected SRC is continuously lit.



Clearing INVcCONF alarms

Alarm clearing action Remove any units that are installed in the wrong slots.



INVcDPLL

Overview

Purpose This section contains information about INVcDPLL alarms.

Organisation This section contains the following information:

- [“INVcDPLL description” \(21-116\)](#)
- [“Clearing INVcDPLL alarms” \(21-117\)](#)



INVcDPLL description

Definition	An INVcDPLL alarm can be caused by an invalid Digital Phase-Locked Loop (DPLL) program. This alarm is activated when a DTU or STU is initialised, and the system discovers an out-of-date DPLL program. This alarm may occur after a software upgrade.
Alarm type	Equipment
Default severity level	You can change the severity level. The default severity level is Deferred for failures that do not affect service.
Local results	A Deferred alarm indicator lights on the following: • User Panel • End-of-suite • Rack-top • Station A red LED on the DTU or STU is continuously lit.



Clearing INVcDPLL alarms

INVcDPLL and INVcFPGA alarms

An FPGA error on the DTU or STU will raise an INVcFPGA alarm. If you get both alarms at once, the following procedure to clear the INVcDPLL alarm will also clear the INVcFPGA alarm.

Before you begin

Make sure all other alarms are cleared before clearing INVcDPLL or INVcFPGA alarms.

Clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).

- 2 Query the protection state for the alarmed unit by doing one of the following:
 - For an STU, perform a query using the MS Control window at *Protection > Equipment > MS Control*.
 - For a DTU, perform a query using the DTU window at *Protection > Equipment > DTU*.

- 3 Does the Unit Status column display Active or Standby?

If	Then
Active	Go to Step 4.
Standby	Go to Step 9.

- 4 Depending on the Current Req value, clear the previous switch request.

Reference: Use one of the following windows:

- *Protection > Equipment > MS Control*
- *Protection > Equipment > DTU*

- 5 Perform another query to verify that the alarmed unit switched to standby.

- 6 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 9.

If	Then
No	The standby unit has also failed. Replace the standby unit and continue to Step 7.

- 7 Perform another query to verify that the alarmed unit switched to standby.

- 8 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 9.
No	Quit this procedure and contact technical support.

- 9 For an STU, use the MS Control window to perform a Freeze.

- 10 Perform a cold start on the standby unit.

It is not necessary to check the Force Reload box. If you check the Force Reload box, the cold start will take longer to complete.

Reference:

For more information, see “Performing a cold start” (11-42).

- 11 Perform a query on the Unit window at *Provision > Equipment > Unit* to verify that the Unit Condition column for the unit now displays Unit provisioned and initialised.

- 12 After performing a cold start on an STU or DTU, monitor the entire system for new alarms. This will ensure that the system has returned to a stable condition, and that any alarms resulting from the loss of clocking have cleared. If an alarm does not clear, clear it with the alarm-clearing procedure for that alarm.

- 13 For an STU, perform a Clear Freeze.

END OF STEPS



INVcFPGA

Overview

Purpose This section contains information about INVcFPGA alarms.

Organisation This section contains the following information:

- “INVcFPGA description” (21-120)
- “Clearing INVcFPGA alarms on a BSC, DTU, or STU” (21-121)
- “Clearing INVcFPGA alarms on port units” (21-123)



INVcFPGA description

Definition	An INVcFPGA alarm can be caused by an invalid Field Programmable Gate Array (FPGA) program. This alarm is activated when units are initialized and the system discovers an out-of-date FPGA program. This alarm may occur after a software upgrade.
Alarm type	Equipment
Default severity level	You can change the severity level. The default severity level is Deferred for failures that do not affect service.
Local results	A Deferred alarm indicator lights on the following: • User Panel • End-of-suite • Rack-top • Station A red LED on any of the following affected units is continuously lit: • BSC • DTU • Port unit • STU



Clearing INVcFPGA alarms on a BSC, DTU, or STU

INVcDPLL and INVcFPGA alarms

If you get an INVcDPLL and an INVcFPGA alarm at the same time, the following procedure to clear the INVcFPGA alarm will also clear the INVcDPLL alarm.

Before you begin

Make sure you clear all other alarms before you clear an INVcFPGA or INVcDPLL alarm.

Clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
- 2 Query the protection state for the alarmed unit by doing one of the following:
 - For an STU or BSC, perform a query using the MS Control window at *Protection > Equipment > MS Control*.
 - For a DTU, perform a query using the DTU window at *Protection > Equipment > DTU*.

- 3 Does the Unit Status column display Active or Standby?

If	Then
Active	Go to Step 4.
Standby	Go to Step 9.

- 4 Depending on the Current Req value, clear the previous switch request.

Reference: Use one of the following windows:

- *Protection > Equipment > MS Control*
- *Protection > Equipment > DTU*

- 5 Perform another query to verify that the alarmed unit switched to standby.

- 6 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 9.

If	Then
No	The standby unit has also failed. Replace the standby unit and continue to Step 7.

- 7 Perform another query to verify that the alarmed unit switched to standby.

- 8 Did the alarmed unit switch to standby?

If	Then
Yes	Go to Step 9.
No	Quit this procedure and contact technical support.

- 9 For an STU or BSC, use the MS Control window to perform a Freeze.

- 10 Perform a cold start on the standby unit.

It is not necessary to check the Force Reload box. If you check the Force Reload box, the cold start will take longer to complete.

Reference:

For more information, see “Performing a cold start” (11-42).

- 11 Perform a query on the Unit window at *Provision > Equipment > Unit* to verify that the Unit Condition column for the unit now displays Unit provisioned and initialised.

- 12 After performing a cold start on an STU, BSC, or DTU, monitor the entire system for new alarms. This will ensure that the system has returned to a stable condition, and that any alarms resulting from the loss of clocking have cleared. If an alarm does not clear, clear it with the alarm-clearing procedure for that alarm.

- 13 For an STU or BSC, perform a Clear Freeze.

END OF STEPS



Clearing INVcFPGA alarms on port units

INVcDPLL and INVcFPGA alarms

If you get an INVcDPLL and an INVcFPGA alarm at the same time, the following procedure to clear the INVcFPGA alarm will also clear the INVcDPLL alarm.

Before you begin

Make sure you clear all other alarms before you clear an INVcFPGA or INVcDPLL alarm.

Clearing actions

The INVcFPGA procedure for clearing alarms on port units is almost identical to clearing Fault-cEQ (FLTcEQ) alarms on port units. However, instead of running a diagnostic test and replacing the unit as stated in the FLTcEQ procedure, cold start the unit.

- 1 Go to one of the following procedures:
 - “Clearing a FLTcEQ on an IU or an unprotected port unit” (21-67)
 - “Clearing a FLTcEQ on an STM-1 electrical unit that uses 1:8 equipment protection” (21-77)
 - “Clearing a FLTcEQ on a port unit that uses NTT MSP” (21-81)
 - “Clearing a FLTcEQ on a port unit that uses SNCP, ITU MSP, or ANSI MSP” (21-85)
-

- 2 Instead of running a diagnostic test and replacing the unit, perform a cold start on the standby unit.

It is not necessary to check the Force Reload box. If you check the Force Reload box, the cold start will take longer to complete.

Reference:

For more information, see “Performing a cold start” (11-42).

- 3 Repeat the procedure for all units.

END OF STEPS



LPcDEG

Overview

Purpose This section contains information about LPcDEG alarms.

Organisation This section contains the following information:

- “LPcDEG description” (21-125)
- “Clearing LPcDEG alarms” (21-126)



LPcDEG description

Definition An LPcDEG alarm indicates a Lower order Path Degraded Bit Error Rate. The equivalent bit error rate of the incoming signal exceeds the provisioned signal degrade threshold.

Alarm type Transmission

Default severity level You can change the severity levels. The default severity levels are as follows:

- Deferred for failures that affect service
- Information for failures that do not affect service

Local results For Deferred alarms, a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

For Information alarms, an Information alarm indicator on the User Panel lights.

For Deferred and Information alarms, the red LED on the affected port unit flashes.



Clearing LPcDEG alarms

Alarm clearing action Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:

- A description of the problem
- A request asking the administrator to examine the relevant upstream equipment



LPcRDI

Overview

Purpose This section contains information about LPcRDI alarms.

Organisation This section contains the following information:

- “LPcRDI description” (21-128)
- “Clearing LPcRDI alarms” (21-129)



LPcRDI description

Definition An LPcRDI alarm indicates a Lower order Path Remote Defect Indicator. The system has received an RDI indication. The downstream equipment has detected transmission that was interrupted at its receive side and is returning RDI.

Alarm type Transmission

Default severity level You can change the severity level. The default severity level is Information for failures that do not affect service.

Local results An Information alarm indicator lights on the User Panel.



Clearing LPcRDI alarms

Alarm clearing actions

- 1 Clear all relevant equipment and transmission alarms that may be active on your own system.

- 2 If the LPcRDI persists, check the local equipment that is connected to the downstream equipment.

END OF STEPS



LPcTIM

Overview

Purpose This section contains information about LPcTIM alarms.

Organisation This section contains the following information:

- “LPcTIM description” (21-131)
- “Clearing LPcTIM alarms” (21-132)



LPcTIM description

Definition An LPcTIM alarm indicates a Lower order Path Trace Identifier Mismatch. The received path trace identifier that is used to verify the continued connection to the intended transmitter does not match the provisioned value.

Incorrect routing exists somewhere in this system or in the upstream direction because:

- Line cables are connected incorrectly or the wrong cross-connections were made upstream
- The Network Element that reported the alarm has the wrong expected Path Trace Identifier (PTI)
- The far-end Network Element has the wrong transmitted PTI

Alarm type Transmission

Default severity level You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected port unit flashes.

Remote results The system does the following in the remote directions:

- Generates an LPaRDI notification in the upstream direction
- Inserts Alarm Indication Signal (AIS) into the transmission signal in the downstream direction



Clearing LPcTIM alarms

Alarm clearing action Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:

- A description of the problem
- A request asking the administrator to examine the relevant upstream equipment



LPcUNEQ

Overview

Purpose This section contains information about LPcUNEQ alarms.

Organisation This section contains the following information:

- “LPcUNEQ description” (21-134)
- “Clearing LPcUNEQ alarms” (21-135)



LPcUNEQ description

Definition	An LPcUNEQ alarm indicates a Lower order Path Unequipped. An LPcUNEQ alarm is activated when the system receives an unequipped signal label. This happens when an intermediate system is provisioned incorrectly and is not transmitting the intended signal.
Alarm type	Transmission
Default severity level	You can change the severity levels. The default severity levels are as follows: • Prompt for failures that affect service • Deferred for failures that do not affect service
Local results	A Prompt or Deferred alarm indicator lights on the following: • User Panel • End-of-suite • Rack-top • Station The red LED on the affected port unit flashes.



Clearing LPcUNEQ alarms

Alarm clearing action Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:

- A description of the problem
- A request asking the administrator to examine the relevant upstream equipment



MCLANcEQ

Overview

Purpose This section contains information about MCLANcEQ alarms.

Organisation This section contains the following information:

- [“MCLANcEQ description” \(21-137\)](#)
- [“MCLANcEQ flowchart” \(21-138\)](#)
- [“Clearing MCLANcEQ alarms” \(21-139\)](#)



MCLANcEQ description

Definition An equipment failure in the Main Controller Local Area Network (MCLAN).

A failure of this type can be caused by any of the following:

- A defective SRC or LHU
- A defective or missing LAN cable
- The removal of a Matrix/Synchronisation or Port Interface subrack's SRC. In this case, the alarm is temporary.

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

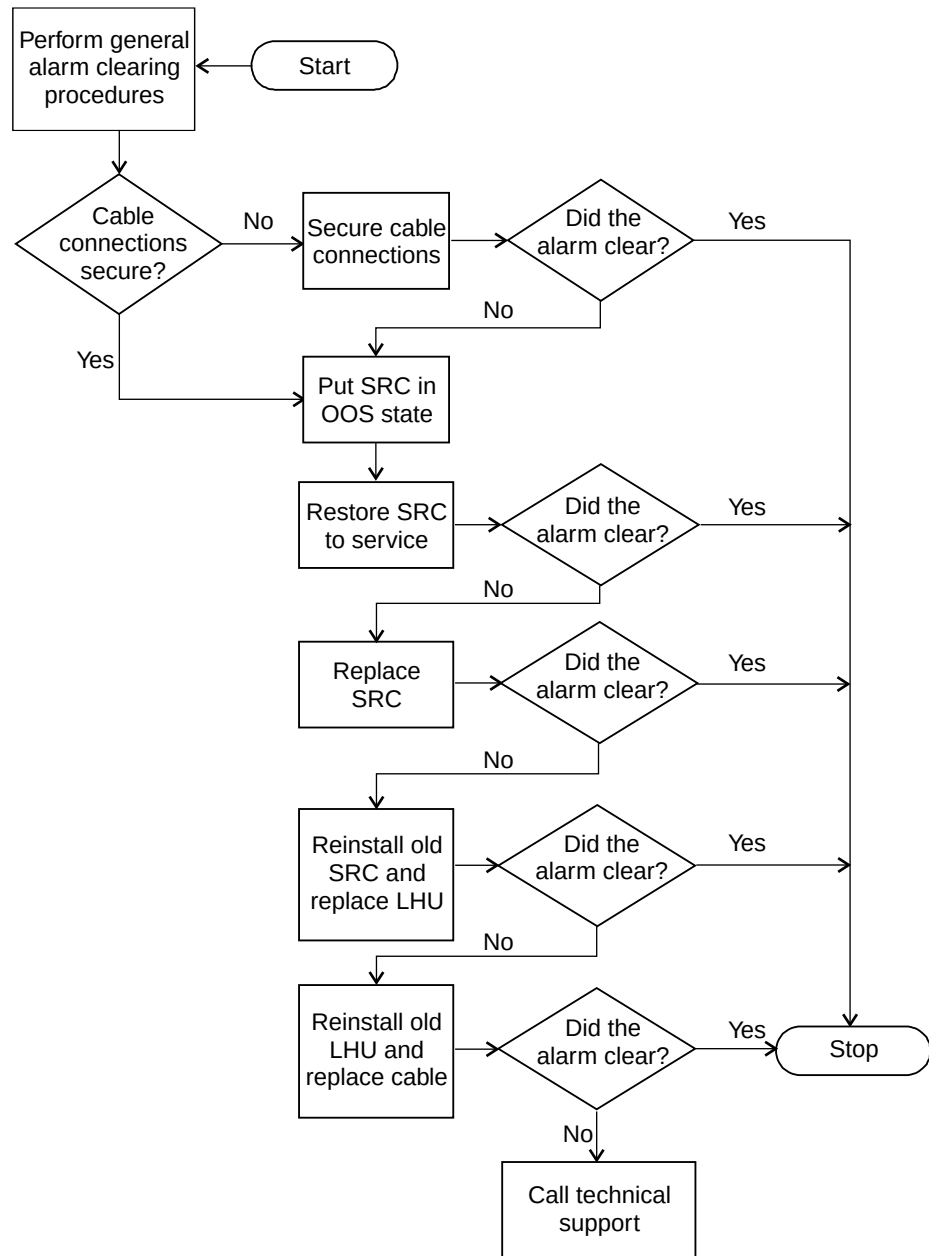
Required equipment Obtain the following equipment to clear the alarm:

- Twisted pair LAN cables
- A new SRC or LHU



MCLANcEQ flowchart

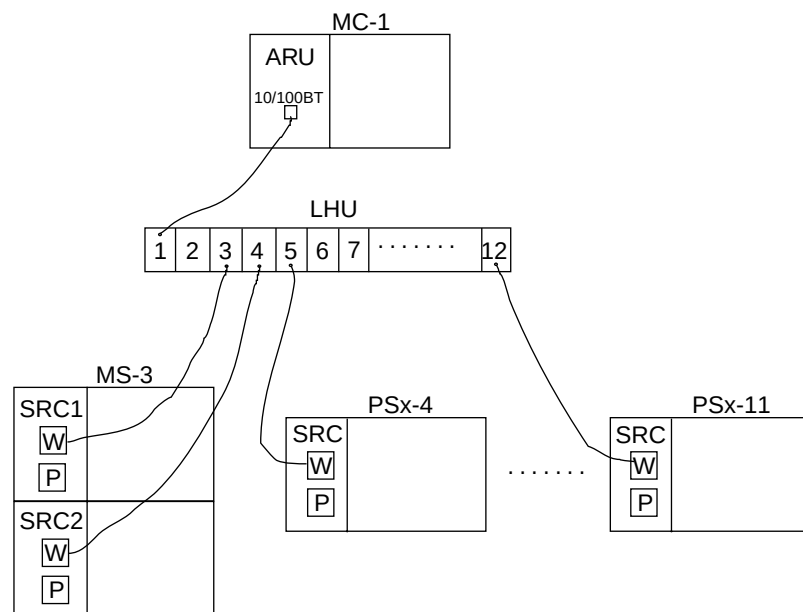
Flowchart The following flowchart shows the procedure for clearing an MCLANcEQ alarm.



Clearing MCLANcEQ alarms

Clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
- 2 To make sure the cable connections are secure, check the connections between the SRC and the LHU. The following figure shows the correct cable connections for one of the two LHUs.



- 3 If the connections were not secure, secure them and wait for the alarm to clear.
- 4 If the connections were secure or the alarm did not clear, place the appropriate SRC in the out-of-service state.

To find the appropriate SRC, you can view the details of the MCLANcEQ alarm from the *Alarms > View Current Alarms* window.

Reference: Use one of the following procedures:

- “Removing a port subrack SRC from service” (11-34)
- “Removing an MS subrack SRC from service” (11-33)

- 5 Restore the SRC to service.

Reference:

Use the procedure in “Restoring an SRC to service” (11-35).

-
- 6 If the alarm does not clear, replace the SRC.
-
- 7 If the alarm still does not clear, reinstall the original SRC and continue with the next step.
-



CAUTION

Do not remove any units without following the appropriate procedures. You could accidentally cause a service interruption, corrupt the hard disk, or power down a subrack and then have to reload the software from the Magneto Optical (MO) disks.

- 8 Replace the LHU.

Reference:

For more information, see “Clearing a FLTcEQ on an ARU, LHU, or PSP” (21-51).

.....

- 9 If the alarm did not clear, replace the unit reporting the alarm by using the appropriate Fault-cEQ (FLTcEQ) procedure.

Reference:

To locate the appropriate FLTcEQ unit-replacement procedure, see “FLTcEQ flowcharts and procedures” (21-48).

.....

- 10 If the alarm still did not clear, reinstall the original LHU and continue with the next step.
-

- 11 Carefully mark the present cable configuration before removing any cables.
-

- 12 Remove both ends of the cable from the modular jacks.
-

- 13 Install a new cable.
-

- 14 If none of these actions clear the alarm, call technical support.

END OF STEPS

.....



MDcIP{1–4}

Overview

Purpose This section contains information about MDcIP{1–4} alarms.

Organisation This section contains the following information:

- “MDcIP{1–4} description” (21-142)
- “Flowchart for clearing an MDcIP{1–4} alarm on a fan in a port rack” (21-143)
- “Clearing an MDcIP{1–4} alarm on a fan in a port rack” (21-144)



MDcIP{1–4} description

Definition An MDcIP{1–4} alarm is associated with each of the Miscellaneous Discrete Inputs (MDIs) 1 through 4. MDIs provide inputs to the DACS system from fan trays in port racks that are equipped with PSC subracks, and from external equipment. You can use MDIs to collect status information from other transmission equipment or to monitor internal and external events such as burglar alarms, smoke detectors, and fan failure alarms. The MDcIP{1–4} alarm is set or cleared according to the state of the miscellaneous discrete input contacts.

Related topic

For more information about MDIs, see “MDIs and MDOs” (6-10).

Miscellaneous discrete input pin assignments MDIs from external equipment are connected to the connector labeled MD IN on the the Fan Connector Panel (FCP). Refer to “Fan Connector Panel (FCP)” (1-25) for a description and illustration of the FCP.

The following table describes the pin assignments on the 25–pin MD IN connector.

MDI	Pins
MDI-1	6 and 18
MDI-2	7 and 19
MDI-3	8 and 20
MDI-4	9 and 21

Alarm type Equipment

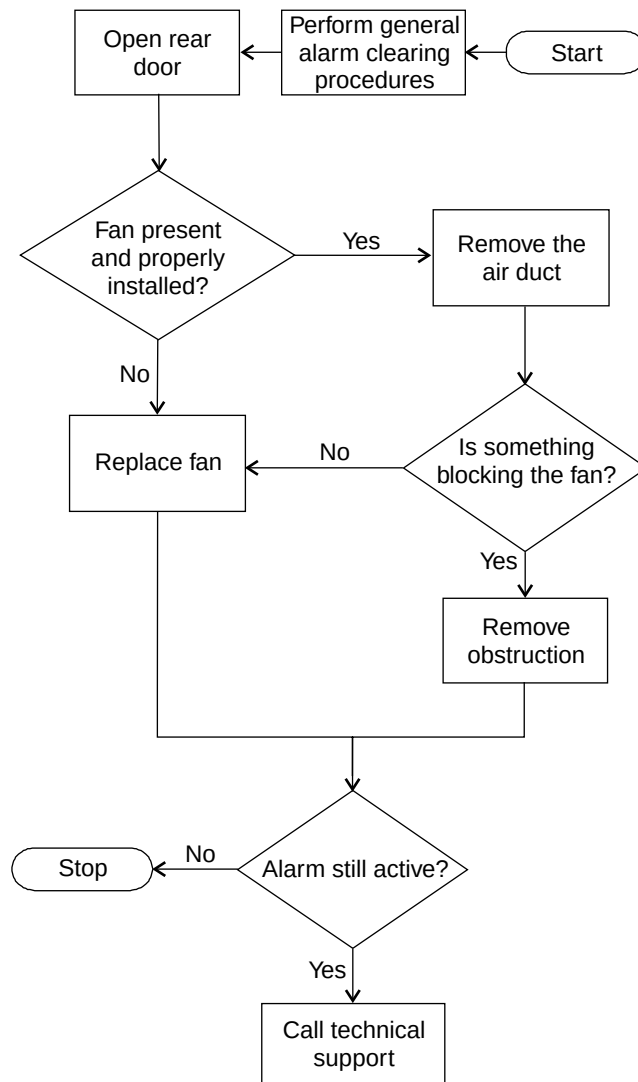
Default severity level You can change the severity level. The default severity level is Information for failures that affect service.

Local results An Information alarm indicator lights on the User Panel.



Flowchart for clearing an MDcIP{1-4} alarm on a fan in a port rack

Flowchart The following flowchart shows the procedure for clearing an MDcIP alarm on a fan in a port rack that is equipped with a PSC subrack.



□

Clearing an MDcIP{1-4} alarm on a fan in a port rack

Clearing actions Check your office records to determine which device is connected to the alarmed MDI, then take the action that is appropriate for your site’s configuration. Use the following procedure to clear an MDcIP{1-4} alarm on a fan in a port rack that is equipped with a PSC subrack:

1 Perform the “General alarm clearing procedure” (21-8).

2 Open the rear door on the port rack, if present.

3 Is the fan physically present and properly installed?

If	Then
Yes	Go to Step 4.
No	Go to Step 8.

4 Remove the air duct that is located above the port rack fan tray.

5 Is something blocking the free flow of air through the fan?

If	Then
Yes	Go to Step 6.
No	Go to Step 8.

6 Remove any obstructions that are restricting free air flow through the fan.

7 Is the alarm still present?

If	Then
Yes	Go to Step 8.
No	Quit this procedure.

8 Remove the fan tray from the rack.

Clearing an MDcIP{1-4} alarm on a fan in
a port rack

.....

9 Slide the new fan tray into the rack.

.....

10 Replace the air duct and the rear door.

.....

11 Return any defective fans to technical support.

Reference:

For more information, see “Procedure for returning defective equipment” (22-5).

.....

END OF STEPS

.....



MScAIS

Overview

Purpose This section contains information about MScAIS alarms.

Organisation This section contains the following information:

- “MScAIS description” (21-147)
- “Clearing MScAIS alarms” (21-148)



MScAIS description

Definition Multiplexer Section (MS) Alarm Indication Signal (AIS). The Multiplexer Section payload signal has been replaced by AIS.

This situation is detected by checking the 6, 7, and 8 bits of the K2 byte for an all “1”s pattern.

This alarm is activated when the system detects a defect in the upstream Network Element.

Alarm type Transmission

Default severity level You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected port unit flashes.

Remote results The system does the following in the remote directions:

- Generates an MSaRDI notification in the upstream direction
- Inserts AIS into the transmission signal in the downstream direction



Clearing MScAIS alarms

Alarm clearing action Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:

- A description of the problem
- A request asking the administrator to examine the relevant upstream equipment



MScDEG

Overview

Purpose This section contains information about MScDEG alarms.

Organisation This section contains the following information:

- “MScDEG description” (21-150)
- “Clearing MScDEG alarms” (21-151)



MScDEG description

Definition Multiplex Section Signal Degrade Threshold Crossing. The bit error rate of the incoming signal exceeds the provisioned signal degrade threshold.

This alarm can be caused by one of the following:

- A fault in the upstream external cabling or the equipment
- An STMcLOS alarm cleared, thereby generating an MScDEG alarm

Alarm type Transmission

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected port unit flashes.



Clearing MScDEG alarms

Alarm clearing actions

- 1 If the problem was a fault in the upstream external cabling or equipment, send a trouble ticket to the network administrator.

The trouble ticket should consist of the following:

- A description of the problem
 - A request asking the administrator to examine the relevant upstream equipment
-

- 2 If the alarm was generated because an STMcLOS alarm cleared, wait the required time for the alarm to clear.

END OF STEPS



MScFOP

Overview

Purpose This section contains information about MScFOP alarms.

Organisation This section contains the following information:

- “MScFOP description” (21-153)
- “Clearing MScFOP alarms” (21-154)



MScFOP description

Definition Multiplex Section (MS) Failure Of Protocol. In a bidirectional mode MSP, the Automatic Protection Switch (APS) signal has detected errors in the protocol information.

This alarm can be caused by any of the following:

- Mismatch of architecture
- Mismatch of line number
- Acknowledge time-out
- Invalid command

Alarm type Transmission

Default severity level You can change the severity level. The default severity level is Prompt for failures that affect service.

Local results A Prompt alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected port unit flashes.



Clearing MScFOP alarms

Alarm clearing action Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:

- A description of the problem
- A request asking the administrator to examine the relevant upstream equipment



MScRDI

Overview

Purpose This section contains information about MScRDI alarms.

Organisation This section contains the following information:

- “MScRDI description” (21-156)
- “Clearing MScRDI alarms” (21-157)



MScRDI description

Definition	Multiplex Section (MS) Remote Defect Indicator (RDI). The system has replaced the MS payload signal with Alarm Indication Signal (AIS), because the downstream equipment has detected AIS transmission at its receive side and is returning RDI.
Alarm type	Transmission
Default severity level	You can change the severity levels. The default severity levels are as follows: • Prompt for failures that affect service • Deferred for failures that do not affect service
Local results	A Prompt or a Deferred alarm indicator lights on the following: • User Panel • End-of-suite • Rack-top • Station The red LED on the affected port unit flashes.



Clearing MScRDI alarms

Alarm clearing actions

- 1 Clear all relevant equipment and transmission alarms that may be active on your own system.

- 2 If the MScRDI alarm persists, check the local equipment that is connected to the downstream equipment.

END OF STEPS



OOScSW

Overview

Purpose This section contains information about OOScSW alarms.

Organisation This section contains the following information:

- “OOScSW description” (21-159)
- “Clearing OOScSW alarms” (21-160)



OOScSW description

Definition The SRC was manually put in the out-of-service maintenance state.

Alarm type Equipment

Default severity level You can change the severity level. The default severity level is Information for failures that affect service, and for failures that do not affect service.

Local results The local results are as follows:

- An Information alarm indicator lights on the User Panel.
- The red LED on the affected SRC is continuously lit.



Clearing OOScSW alarms

Clearing actions

- 1 Click on Current Alarms on the Alarm Panel and record the software address of the SRC with the OOScSW alarm.

- 2 Restore the SRC to service.

Reference:

Use the procedure in “Restoring an SRC to service” (11-35).

END OF STEPS



POWcDEG

Overview

Purpose This section contains information about POWcDEG alarms.

Organisation This section contains the following information:

- “POWcDEG description” (21-162)
- “Battery power” (21-163)
- “Clearing POWcDEG alarms” (21-164)



POWcDEG description

Definition A POWcDEG alarm can be caused by either a battery power failure or a fuse failure.

The battery or fuse failure can involve any of the following:

- Main Controller subrack Power Supply (PSP) (battery power failures only)
- Matrix and Synchronisation subrack Power Terminal Module (PTM)
- PSA PTM
- PSC PTM

Related topic

For more information, see “Battery power” (21-163).

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

If the cause of the alarm is low battery power or a battery failure, no red fail LED will be lit on any of the PTMs, and no green power LED will be lit on the PSP.

If the cause of the alarm is a fuse failure in the PTM, the red LED on that PTM will be continuously lit.

Required equipment For alarms associated with a PTM fuse failure, obtain a new 20-amp fuse of the same type.



Battery power

About battery power

A POWcDEG alarm can mean a battery power failure directly to a BSSU.

Station battery power (nominally, –48 volts) is expected to be supplied from dual sources. This power is wired to dual PTMs. Each of the dual PTMs has a D-sub power connector. Dual power modules in the Main Controller subrack have a common terminal block for dual power, and the BSSU has one D-sub power connector for dual power.



Clearing POWcDEG alarms

Clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
- 2 Based on the rack-top address and other information obtained during the general alarm clearing procedures, locate the rack that contains the affected unit.
- 3 Open the rack doors.
- 4 Remove the Electromagnetic Compliance (EMC) shields as necessary from the subracks so you can examine the unit LEDs.
- 5 Is a red fail LED lit on any of the PTMs, or is the green power LED not lit on the PSP?

If	Then
There is no red fail LED lit on a PTM, or if there is no green power LED lit on the PSP.	There is a battery power failure. Go to “Clearing a battery power failure” (21-165).
The red fail LED on a PTM is continuously lit.	There is a blown fuse for that PTM. Go to “Replacing a blown fuse” (21-165).

END OF STEPS

Clearing a battery power failure

- 1 Make sure the rack-top power A and power B line connections are secure.
- 2 Make sure the 8-mm lugs on the rack-top are tight.
- 3 If all the connections are secure and tight, use local office procedures to replace the office battery or the wiring from the office battery.
- 4 If the alarm still does not clear, contact technical support for assistance.

END OF STEPS

Replacing a blown fuse

- 1 Locate the fuse that corresponds to the lit LED.
- 2 Remove the PTM fuse holder containing the defective fuse by turning the fuse holder counterclockwise.
- 3 Remove the fuse from its holder.
- 4 Obtain a 20-amp replacement fuse of the same type as the blown fuse.
- 5 Insert the replacement fuse into the fuse holder.
- 6 Reinsert the fuse holder containing the new fuse by turning the fuse holder clockwise.
- 7 Reinstall the EMC shields that you removed.
- 8 Close the rack doors.
- 9 If the alarm fails to clear, or if the same fuse blows again, contact technical support.

END OF STEPS



RScLOF

Overview

Purpose This section contains information about RScLOF alarms.

Organisation This section contains the following information:

- “RScLOF description” (21-167)
- “Clearing RScLOF alarms” (21-168)



RScLOF description

Definition Regenerator Section (RS) Loss of Synchronous Transport Module (STM) Frame. Alignment to the frame structure of the received signal is not possible. Therefore, the system cannot extract Multiplexer Section (MS) and Virtual Container (VC) overhead and payload data.

This alarm can be caused by one of the following:

- An equipment fault in the upstream or local office
- Defective cabling

Alarm type Transmission

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected port unit flashes.

Remote results The system does the following in the remote directions:

- Generates an MSaRDI notification in the upstream direction
- Inserts Alarm Indication Signal (AIS) into the transmission signal in the downstream direction



Clearing RScLOF alarms

Alarm clearing actions

- 1** Check the network management system to see if a unit failure has been reported for the unit generating the frame alignment signal.

- 2** In the appropriate Network Element, remove the unit and replace it with a new one.

- 3** In case a unit failure is not reported, loop the signal at the transmitting Network Element and at the receiving Network Element. In this condition, the Network Element reporting STM-(N) Loss of Frame (LOF) contains the faulty unit.

- 4** Check the intermediate cabling.

END OF STEPS



STMcLOS

Overview

Purpose This section contains information about STMcLOS alarms.

Organisation This section contains the following information:

- “STMcLOS description” (21-170)
- “Clearing STMcLOS alarms” (21-171)



STMcLOS description

Definition Loss of Electrical or Optical Incoming Synchronous Transfer Module (STM) Signal. The power level of the received signal is so low that the system is unable to recognize whether the signal has an STM-(N) frame structure.

This alarm can be caused by any of the following:

- Cable rupture
- Dirty optical connectors
- Equipment failures in the upstream Network Element that reported the alarm

Alarm type Transmission

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected port unit flashes.

Remote results The system does the following in the remote directions:

- Generates an MSaRDI notification in the upstream direction
- Inserts Alarm Indication Signal (AIS) into the transmission signal in the downstream direction



Clearing STMcLOS alarms

Alarm clearing actions

- 1** Check for cable breaks.

- 2** If any cable breaks are found, replace the cable and wait for the alarm to clear.

- 3** If no cable breaks are found, clean the optical connectors and wait for the alarm to clear.

Result:

When an STMcLOS alarm clears for the port unit, the system may activate an MScDEG alarm. The MScDEG alarm will clear automatically.

END OF STEPS



SYNCcCCRF

Overview

Purpose This section contains information about SYNCcCCRF alarms.

Organisation This section contains the following information:

- [“SYNCcCCRF description” \(21-173\)](#)
- [“Possible causes of a SYNCcCCRF alarm” \(21-174\)](#)
- [“SYNCcCCRF flowchart” \(21-175\)](#)
- [“Clearing SYNCcCCRF alarms” \(21-176\)](#)



SYNCcCCRF description

Definition A SYNCcCCRF alarm is a Cross-Couple Reference Failure between the active and standby System Timing Units (STUs). This alarm is always raised on the standby STU.

Related topic

For more information, see “Possible causes of a SYNCcCCRF alarm” (21-174).

Alarm type Equipment

Default severity level You can change the severity level. The default severity level is Deferred for failures that do not affect service.

Local results A Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

Required equipment The following equipment may be required:

- STU
- BSC
- OLU
- Cable(s) between the OLUs



Possible causes of a SYNCCCRF alarm

What caused the alarm? The SYNCCCRF alarm indicates that there is a problem with either the cross-couple communication link or the cross-couple timing link between the STUs. The Equipment ID in the alarm message will tell you if the XCOUPLE-TIME or the XCOUPLE-COMM link has the problem.

Possible XCOUPLE-COMM problems For the cross-couple communication link, the alarm can be caused by the following:

- A failure in an STU
- A failure in a BSC
- A failure in an OLU (OLU1 or OLU3)
- Missing or defective cables between the OLUs
- Defective backplane connection from the STU to the BSC

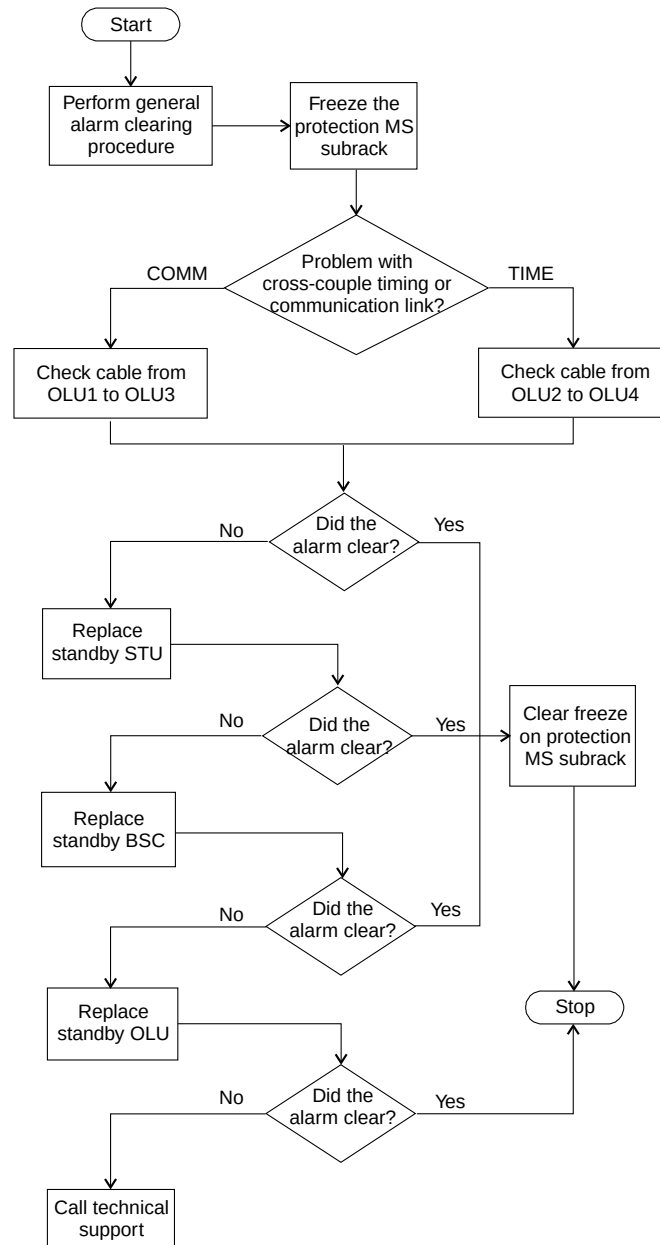
Possible XCOUPLE-TIME problems For the cross-couple timing link, the alarm can be caused by the following:

- A failure in an STU
- A failure in a BSC
- A failure in an OLU (OLU2 or OLU4)
- Missing or defective cables between the OLUs
- Defective backplane connection from the STU to the BSC



SYNCcCCRF flowchart

Flowchart The following flowchart shows the procedure for clearing a SYNCcCCRF alarm.



□

Clearing SYNCCCRF alarms

Alarm clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).

- 2 Freeze the protection Matrix and Synchronisation subrack.

Reference:

Use the MS Control window at *Protection > Equipment > MS Control*.

- 3 Is there a problem with the cross-couple communication link or the cross-couple timing link?

If	Then
The problem is in the cross-couple communication link	Verify that the cross-couple cable connecting port 6 of OLU1 to OLU3 is installed properly.
The problem is in the cross-couple timing link	Verify that the cross-couple cable connecting port 6 of OLU2 to OLU4 is installed properly.

- 4 If the alarm does not clear, replace the standby STU.

Reference:

For more information, see “Clearing a FLTcEQ on a BSC or STU” (21-53).

- 5 If the alarm does not clear, replace the standby BSC.

Reference:

For more information, see “Clearing a FLTcEQ on a BSC or STU” (21-53).

- 6 If the alarm does not clear, replace the standby OLU.

Reference:

For more information, see “Clearing a FLTcEQ on an OLU” (21-72).

7 Did the alarm clear?

If	Then
The alarm clears	Clear the freeze on the protection Matrix and Synchronisation subrack. Reference: Use the MS Control window at <i>Protection > Equipment > MS Control</i> .
The alarm does not clear	Call technical support.

END OF STEPS



SYNCcLTRF

Overview

Purpose This section contains information about SYNCcLTRF alarms.

Organisation This section contains the following information:

- “SYNCcLTRF description” (21-179)
- “SYNCcLTRF flowchart” (21-180)
- “Clearing SYNCcLTRF alarms” (21-182)



SYNCCLTRF description

Definition Line Timing Reference Failure. The input timing reference for the system clock, station clock output, or both are derived from a transmission port, and there is a problem with the signal. This alarm is always raised on the transmission port that is providing the timing reference.

This alarm can be caused by any of the following:

- A failure in the incoming signal to the transmission port
- A failure in the transmission port
- A failure in an internal transmission path between the port and the STU

Alarm type Transmission

Default severity level You can change the severity level. The default severity level is Deferred for failures that do not affect service.

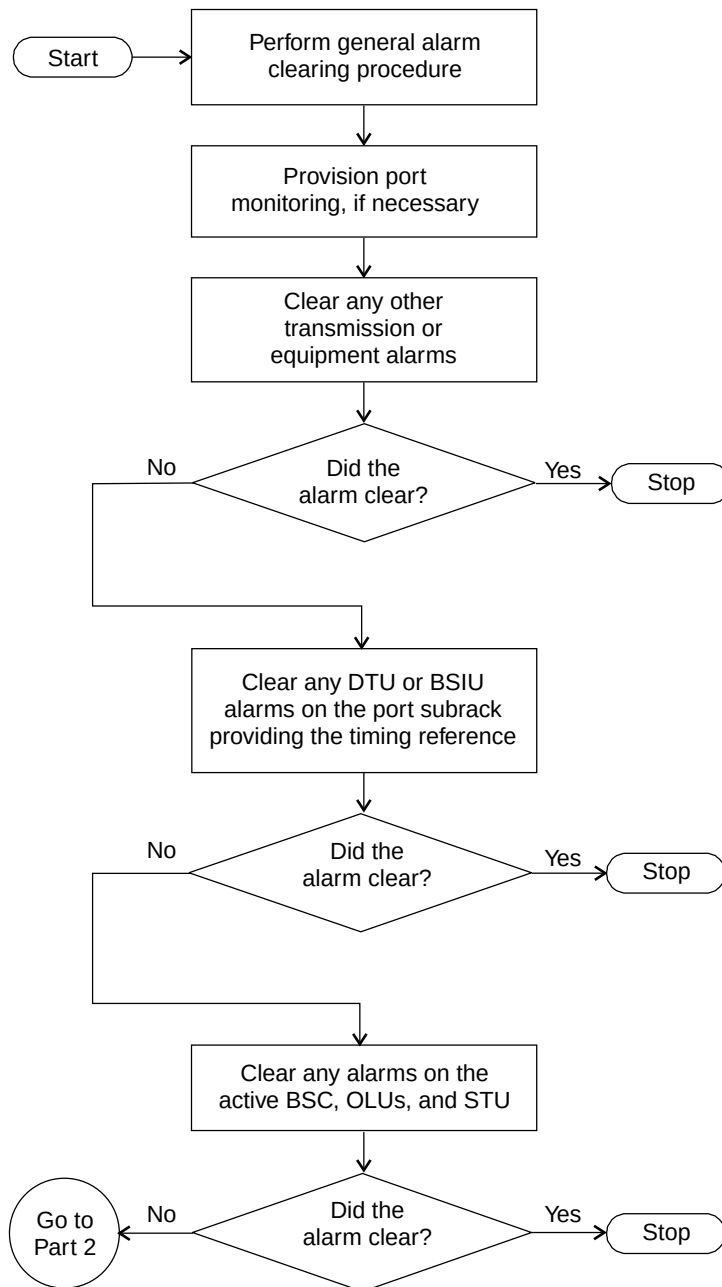
Local results A Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

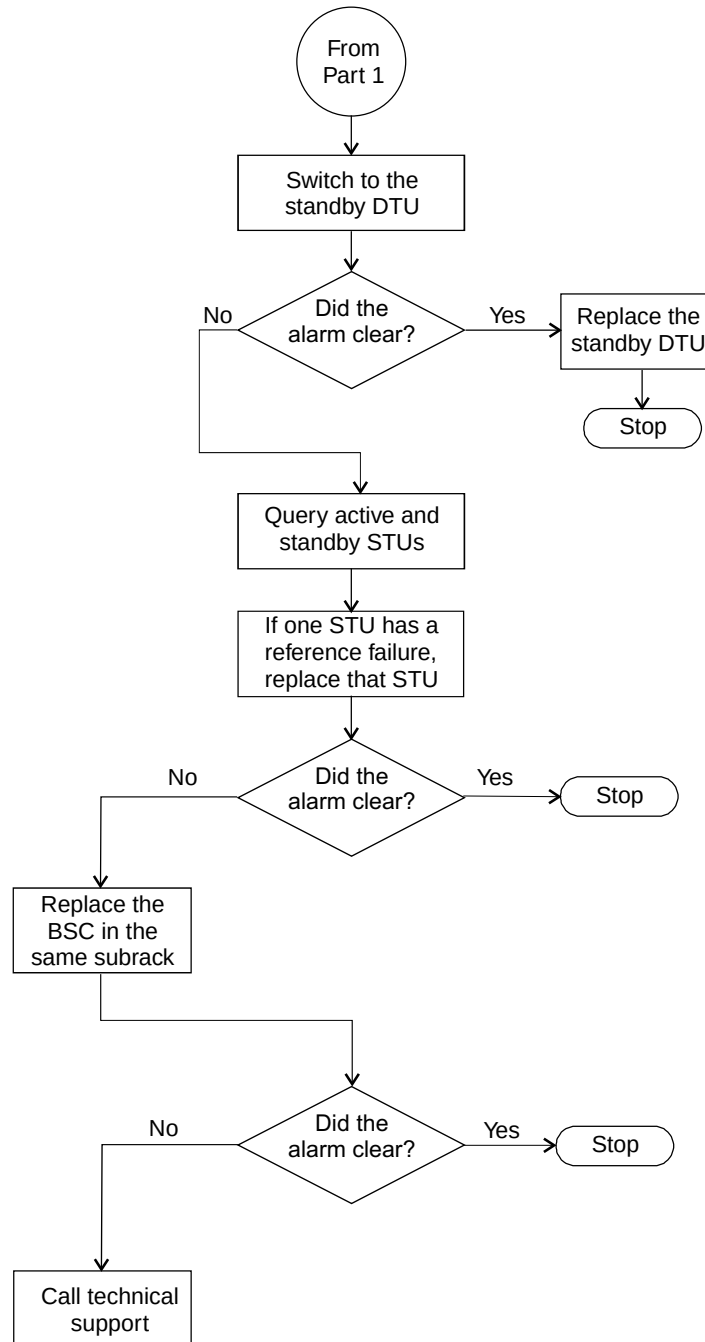


SYNCcLTRF flowchart

Flowchart, part 1 The following flowchart shows part 1 of the procedure for clearing a SYNCcLTRF alarm.



Flowchart, part 2 The following flowchart shows part 2 of the procedure for clearing a SYNCcLTRF alarm.



□

Clearing SYNCcLTRF alarms

Alarm clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
-

- 2 Verify that the port that is providing the input timing reference is being monitored for defects and alarms.

Reference:

Query the port using the Port Monitoring window at *Provision > Monitoring Control > Port Monitoring*.

- 3 If the port is not being monitored for defects and alarms, assign port monitoring.

Reference:

Use the Port Monitoring window.

- 4 If the SYNCcLTRF alarm did not clear, check for a transmission (STMcLOS or MScAIS) or equipment (FLTcEQ) alarms on the port that is providing the input timing reference.

Reference:

Query the active alarms using the View Current Alarms window at *Alarms > View Current Alarms*.

- 5 If alarms are present, clear them using the appropriate alarm-clearing procedure.

Example:

For an alarm on the STU, use “Clearing a FLTcEQ on a BSC or STU” (21-53).

- 6 If the SYNCcLTRF alarm did not clear, check for DTU or BSIU alarms on the port subrack that is providing the input timing reference.

Reference:

Use the View Current Alarms window.

.....

7 If alarms are present, clear them using the appropriate alarm-clearing procedure.

.....

8 If the SYNCcLTRF alarm did not clear, check for equipment alarms on the active BSC, OLUs, and STU using the View Current Alarms window.

.....

9 If alarms are present, clear them using the appropriate alarm-clearing procedure.

.....

10 If the SYNCcLTRF alarm did not clear, switch to the standby DTU.

Reference:

Use the DTU window at *Protection > Equipment > DTU*.

.....

11 Did the alarm clear?

If	Then
The alarm clears	Replace the standby DTU. Reference: For more information, see “Clearing a FLTcEQ on a DTU” (21-61).
The alarm does not clear	Query the active and standby STUs. Reference: Use the System Clock window at <i>Provision > Synchronisation and Timing > System Clock</i> .

.....

12 If one STU has a reference failure, replace that STU.

.....

13 If the SYNCcLTRF alarm did not clear, replace the BSC in the same subrack.

.....

14 If the SYNCcLTRF alarm did not clear, call technical support.

END OF STEPS

.....



SYNCcROOR

Overview

Purpose This section contains information about SYNCcROOR alarms.

Organisation This section contains the following information:

- “SYNCcROOR description” (21-185)
- “Clearing SYNCcROOR alarms” (21-186)



SYNCCROOR description

Definition Reference Out Of Range. The frequency of an input timing reference is outside the allowed range. This alarm is always raised on the transmission port or the station clock that is providing the timing reference.

This alarm can be caused by one of the following:

- A failure in an STU
- A timing loop in the synchronisation network

Alarm type Transmission

Default severity level You can change the severity level. The default severity level is Deferred for failures that do not affect service.

Local results A Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

Required equipment An STU may be required.



Clearing SYNCcROOR alarms

Alarm clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
- 2 Check the signal level and frequency of the input reference using local office procedures.
- 3 Does the input reference signal meet the ITU-T G.703 recommendation?

If	Then
The reference signal does not meet the ITU-T recommendation	Delete the timing reference.
The reference signal meets the ITU-T recommendation	The STU is defective. Replace it using the procedure in “Clearing a FLTcEQ on a BSC or STU” (21-53).

- 4 If the alarm does not clear, call technical support.

END OF STEPS



SYNCcSCF

Overview

Purpose This section contains information about SYNCcSCF alarms.

Organisation This section contains the following information:

- “SYNCcSCF description” (21-188)
- “Clearing SYNCcSCF alarms” (21-189)



SYNCCSCF description

Definition A System Clock Failure. This internal type of failure may prevent the system clock from operating.

This type of alarm can be caused by a failure in an STU.

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected STU is continuously lit.

Required equipment Obtain a new STU.



Clearing SYNCCSCF alarms

Alarm clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
-

- 2 Replace the STU.

Reference:

Use the procedure in “Clearing a FLTcEQ on a BSC or STU” (21-53).

END OF STEPS



SYNCcSCHO

Overview

Purpose This section contains information about SYNCcSCHO alarms.

Organisation This section contains the following information:

- “SYNCcSCHO description” (21-191)
- “Clearing SYNCcSCHO alarms” (21-192)



SYNCcSCHO description

Definition A SYNCcSCHO alarm is generated whenever the system timing mode changes to holdover.

The system timing mode can change to holdover for any of the following reasons:

- All provisioned timing references have failed
- Maintenance personnel have manually switched the timing mode to holdover to work on a timing reference
- No timing references are provisioned, and a protection switch of Matrix and Synchronisation control has occurred

A SYNCcSCHO alarm is also generated during automatic or manual switching of Matrix and Synchronisation control. If one or more timing references are provisioned, the alarm should be temporary.

Alarm type Equipment

Default severity level You can change the severity level. The default severity level is Deferred for failures that do not affect service.

Local results A Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station



Clearing SYNCcSCHO alarms

Alarm clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
-

- 2 Clear any SYNCcLTRF or SYNCcSTCRF alarms first.

Reference:

Use the procedures in “Clearing SYNCcLTRF alarms” (21-182) and/or “Clearing SYNCcSTCRF alarms” (21-200).

- 3 Assign the station clock or a transmission port as a timing reference for the system clock.

Reference:

Go to *Provision > Synchronisation and Timing > System Clock*.

- 4 Verify that the priority assigned to the internal clock is less than any provisioned timing reference.

Reference:

Query the system clock using the System Clock window.

- 5 If the priority assigned to the system clock is not less than any provisioned timing reference, lower the priority of the system clock.

END OF STEPS



SYNCcSTCOF

Overview

Purpose This section contains information about SYNCcSTCOF alarms.

Organisation This section contains the following information:

- “SYNCcSTCOF description” (21-194)
- “SYNCcSTCOF flowchart” (21-195)
- “Clearing SYNCcSTCOF alarms” (21-196)



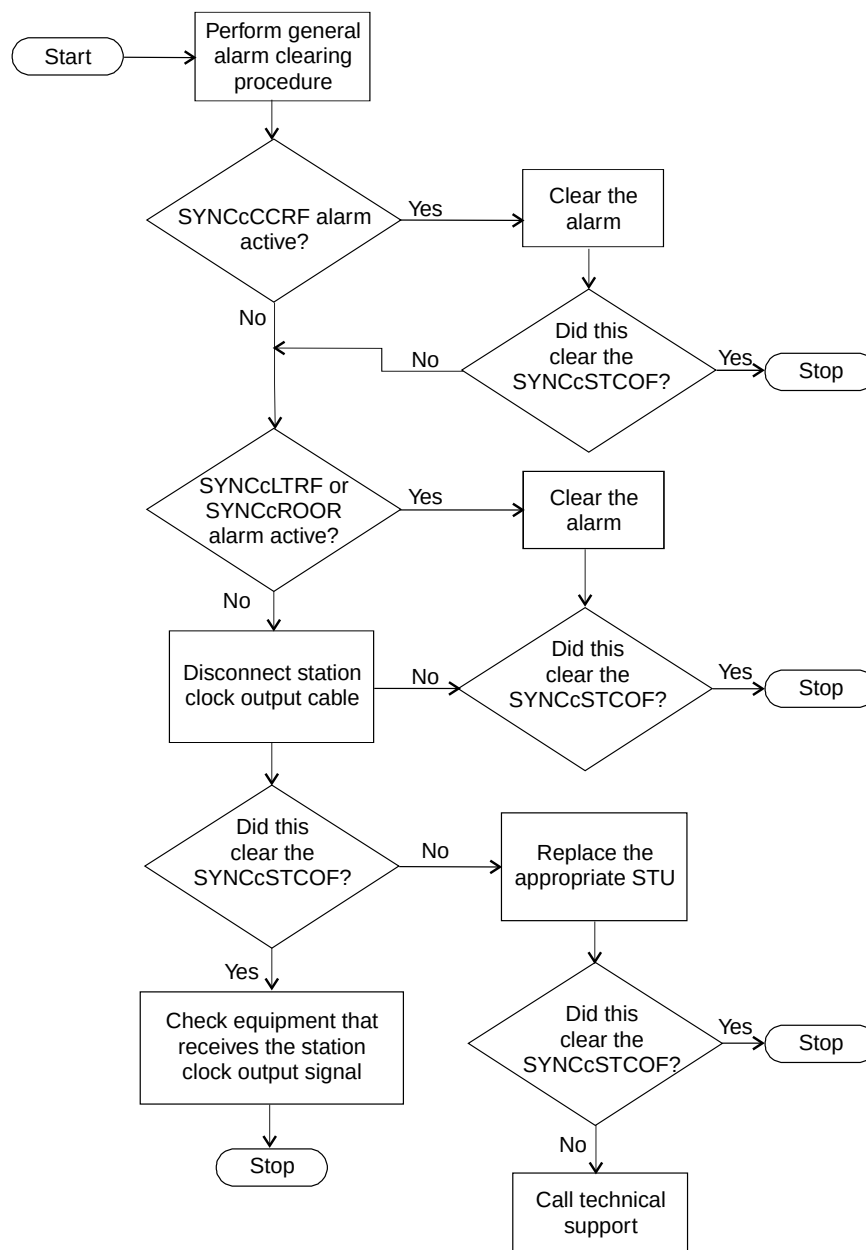
SYNCcSTCOF description

Definition	This alarm is associated with a station clock output failure. This alarm can be caused by any of the following: • A failure of the input signal when the station clock output is derived from a transmission port (line-derived timing) • An improperly terminated load (for example: the output cable is shorted or not terminated at the recipient Network Element) • A SYNCcSCE, SYNCcCCRF, or Fault-cEQ (FLTcEQ) alarm on an STU • A failure in an STU
Alarm type	Equipment
Default severity level	You can change the severity level. The default severity level is Information for failures that do not affect service.
Local results	An Information alarm indicator lights on the User Panel.
Required equipment	An STU may be required.



SYNCcSTCOF flowchart

Flowchart The following flowchart shows the procedure for clearing a SYNCcSTCOF alarm.



□

Clearing SYNCcSTCOF alarms

Alarm clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
-

- 2 Check for a SYNCcCCRF alarm.

Reference:

Use the View Current Alarms window at *Alarms > View Current Alarms*.

- 3 Clear the SYNCcCCRF alarm first.

Reference:

For more information, see “Clearing SYNCcCCRF alarms” (21-176)

- 4 If clearing the SYNCcCCRF alarm did not clear the SYNCcSTCOF alarm, check for a SYNCcLTRF or SYNCcROOR alarm.

Reference:

Use the View Current Alarms window.

- 5 Clear any SYNCcLTRF or SYNCcROOR alarms, if necessary.

Reference: For more information, see one of the following topics:

- “Clearing SYNCcLTRF alarms” (21-182)
 - “Clearing SYNCcROOR alarms” (21-186)
-

- 6 If clearing the SYNCcLTRF or SYNCcROOR alarms did not clear the SYNCcSTCOF alarm, disconnect the station clock output cable.
-

- 7 If the SYNCcSTCOF alarm did not clear, replace the STU identified in the alarm message.

Reference:

For more information, see “Clearing a FLTcEQ on a BSC or STU” (21-53).

.....

8 Did the SYNCcSTCOF alarm clear?

If	Then
The SYNCcSTCOF alarm cleared	Check the equipment that is receiving the station clock output signal.
The SYNCcSTCOF alarm did not clear	Replace the STU identified in the alarm message using the procedure in “Clearing a FLTcEQ on a BSC or STU” (21-53).

.....

9 If the SYNCcSTCOF alarm did not clear, call technical support.

END OF STEPS

.....



SYNCcSTCRF

Overview

Purpose This section contains information about SYNCcSTCRF alarms.

Organisation This section contains the following information:

- “SYNCcSTCRF description” (21-199)
- “Clearing SYNCcSTCRF alarms” (21-200)



SYNCCSTCRF description

Definition	Station Clock Reference Failure. This alarm is associated with a failure of a station clock input (Station-Clock-In-1 or Station-Clock-In-2), and is always raised on the active STU. The Equipment ID in the alarm message will identify the input that has the failure.
Alarm type	Transmission
Default severity level	You can change the severity level. The default severity level is Deferred for failures that do not affect service.
Local results	A Deferred alarm indicator lights on the following: • User Panel • End-of-suite • Rack-top • Station The red LED on the affected STU flashes.
Required equipment	An STU or a station clock input cable may be required.



Clearing SYNCcSTCRF alarms

Alarm clearing actions

- 1 Perform the “General alarm clearing procedure” (21-8).
- 2 Check the station clock input cable and replace if necessary.
- 3 If the SYNCcSTCRF alarm did not clear, check the signal level and frequency of the input reference using local office procedures.
- 4 Does the reference signal meet the ITU-T recommendation?

If	Then
The reference signal does <i>not</i> meet the ITU-T recommendation	Go to Step 5.
The reference signal meets the ITU-T recommendation	Go to Step 6.

- 5 Delete the timing reference or assign it the priority None.
Go to Step 8.

Reference:

Use the System Clock window at *Provision > Synchronisation and Timing > System Clock*.

- 6 Query the system clock.

Reference:

Use the System Clock window at *Provision > Synchronisation and Timing > System Clock*.

- 7 Replace the STU that reports an input failure.

Reference:

For more information, see “Clearing a FLTcEQ on a BSC or STU” (21-53).

- 8 If the alarm does not clear, call technical support.

END OF STEPS



TEMPcEQ

Overview

Purpose This section contains information about TEMPcEQ alarms.

Organisation This section contains the following information:

- “TEMPcEQ description” (21-202)
- “Clearing TEMPcEQ alarms” (21-203)



TEMPcEQ description

Definition The temperature of a unit is too high. This alarm will *not* cause a protection switch.

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

An Information LED is continuously lit on the port unit, or on the Interface Unit (IU).

Required equipment Obtain a new unit.



Clearing TEMPcEQ alarms

Alarm clearing actions

- 1 Check for system environmental conditions that could be causing high temperatures (for example: defective air conditioning).
-



CAUTION

Do not remove any units without following the appropriate procedures. You could accidentally cause a service interruption, corrupt the hard disk, or power down a subrack and then have to reload the software from the Magneto Optical (MO) disks.

- 2 If high temperature in the equipment room is not the problem, replace the port unit or IU by using the appropriate Fault-cEQ (FLTcEQ) procedure.

Reference: For more information, see one of the following procedures:

- “Clearing a FLTcEQ on an IU or an unprotected port unit” (21-67)
- “Clearing a FLTcEQ on an STM-1 electrical unit that uses 1:8 equipment protection” (21-77)
- “Clearing a FLTcEQ on a port unit that uses NTT MSP” (21-81)
- “Clearing a FLTcEQ on a port unit that uses SNCP, ITU MSP, or ANSI MSP” (21-85)

END OF STEPS



TUcAIS

Overview

Purpose This section contains information about TUcAIS alarms.

Organisation This section contains the following information:

- “TUcAIS description” (21-205)
- “Clearing TUcAIS alarms” (21-206)



TUcAIS description

Definition Tributary Unit Alarm Indication Signal (AIS). The system has replaced the VC-12 or VC-3 payload signal with AIS. The upstream Network Element or an upstream function in the system has detected a defect which led to the insertion of AIS.

Alarm type Transmission

Default severity level You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Information for failures that do not affect service

Local results For Prompt alarms, a Prompt alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

For Information alarms, an Information alarm indicator on the User Panel lights.

For Prompt and Information alarms, the red LED on the affected port unit flashes.

Remote results The system does the following in the remote directions:

- Generates an LPaRDI notification in the upstream direction
- Inserts Alarm Indication Signal (AIS) into the transmission signal in the downstream direction



Clearing TUCAIS alarms

Alarm clearing action Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:

- A description of the problem
- A request asking the administrator to examine the relevant upstream Plesiochronous Digital Hierarchy (PDH) equipment



TUcLOM

Overview

Purpose This section contains information about TUcLOM alarms.

Organisation This section contains the following information:

- “TUcLOM description” (21-208)
- “Clearing TUcLOM alarms” (21-209)



TUcLOM description

Definition	Tributary Unit Loss of Multiframe. Alignment to the multiframe structure of the received VC-4 signal is not possible. Therefore, the system cannot extract the VC-12 overhead and payload data. This alarm can be caused by a unit failure in the upstream Network Element that generated the H4 multiframe alignment signal or in the Network Element that reported the alarm.
Alarm type	Transmission
Default severity level	You can change the severity levels. The default severity levels are as follows: • Prompt for failures that affect service • Deferred for failures that do not affect service
Local results	A Prompt or a Deferred alarm indicator lights on the following: • User Panel • End-of-suite • Rack-top • Station The red LED on the affected port unit flashes.
Remote results	The system inserts Alarm Indication Signal (AIS) into the transmission signal in the downstream direction.



Clearing TUcLOM alarms

Alarm clearing action Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:

- A description of the problem
- A request asking the administrator to examine the relevant upstream equipment



TUcLOP

Overview

Purpose This section contains information about TUcLOP alarms.

Organisation This section contains the following information:

- “TUcLOP description” (21-211)
- “Clearing TUcLOP alarms” (21-212)



TUcLOP description

Definition Tributary Unit Loss of Pointer. The system could not obtain a valid TU pointer interpretation in the received signal.

A unit has failed in the upstream Network Element that generated the TU pointer or in the Network Element that reported the alarm.

Alarm type Transmission

Default severity level You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected port unit flashes.

Remote results The system does the following in the remote directions:

- Generates an LPaRDI notification in the upstream direction
- Inserts Alarm Indication Signal (AIS) into the transmission signal in the downstream direction



Clearing TUcLOP alarms

Alarm clearing action Send a trouble ticket to the network administrator. The trouble ticket should consist of the following:

- A description of the problem
- A request asking the administrator to examine the relevant upstream equipment.



UNIceEQ

Overview

Purpose This section contains information about UNIceEQ alarms.

Organisation This section contains the following information:

- “UNIceEQ description” (21-214)
- “Clearing UNIceEQ alarms for most cases” (21-215)
- “Clearing UNIceEQ alarms when the alarm appears after SRC insertion” (21-216)
- “Clearing UNIceEQ alarms when the alarm is raised against a BSSU” (21-217)



UNICeQ description

Definition Unit Not Installed. The system will generate this alarm when a provisioned unit is not installed or when the system cannot communicate with the unit.

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

- User Panel
- End-of-suite
- Rack-top
- Station



Clearing UNICeQ alarms for most cases

General clearing actions

Do one of the following:

- Insert the appropriate unit in the proper slot.
- If you do not want a unit in that particular slot, and the alarmed unit is a port unit, delete the unit using the Unit window at *Provision > Equipment > Unit*.



Clearing UNiCeq alarms when the alarm appears after SRC insertion

Clearing action **Important!** The system may generate a UNiCeq alarm after an SRC is inserted and before it begins to boot. After a few minutes, the system will begin to boot the SRC, and the UNiCeq alarm will clear. If the alarm persists after the SRC has begun to boot, check the cabling.



Clearing UNICeQ alarms when the alarm is raised against a BSSU

Clearing action If the UNICeQ alarm is raised against the BSSU, the alarm may be caused by an improperly-connected optical cable from the BSSU to the OLU on the active side of the Matrix and Synchronisation subrack.

If the BSSU is present, check both the power cable and the optical cable connections to clear the alarm.



VOLcDI

Overview

Purpose This section contains information about VOLcDI alarms.

Organisation This section contains the following information:

- “VOLcDI description” (21-219)
- “Clearing VOLcDI alarms” (21-220)



VOLcDI description

Definition A Volatile Data Integrity failure. This alarm is generated when an audit reveals that database data has failed.

Important! A VOLcDI alarm is activated only on the Main Controller subrack.

Alarm type Equipment

Default severity level You can change the severity level. The default severity level is Information for failures that do not affect service.

Local results An Information alarm indicator lights on the User Panel.



Clearing VOLcDI alarms

Alarm clearing action Call technical support to resolve this alarm.



VOLcREP

Overview

Purpose This section contains information about VOLcREP alarms.

Organisation This section contains the following information:

- “VOLcREP description” (21-222)
- “Clearing VOLcREP alarms” (21-223)



VOLcREP description

Definition A Volatile Data Replication failure. This alarm applies only to systems that have a duplicated MC. The VOLcREP alarm is generated when the system detects that database information is not being copied from the active MC to the standby MC.

Alarm type Equipment

Default severity level You can change the severity level. The default severity level is Deferred for failures that do not affect service.

Local results An Deferred alarm indicator lights on the User Panel.



Clearing VOLcREP alarms

Alarm clearing action Call technical support to resolve this alarm.



WUPcEQ

Overview

Purpose This section contains information about WUPcEQ alarms.

Organisation This section contains the following information:

- “WUPcEQ description” (21-225)
- “WUPcEQ flowchart” (21-226)
- “Clearing WUPcEQ alarms for SRC units” (21-227)
- “Clearing WUPcEQ alarms for all units except SRC units” (21-228)



WUPcEQ description

Definition Wrong Unit Present. This alarm can be caused by either of the following problems:

- An incorrect version of a unit has been inserted.
- The wrong unit type has been inserted.

Alarm type Equipment

Default severity levels You can change the severity levels. The default severity levels are as follows:

- Prompt for failures that affect service
- Deferred for failures that do not affect service

Local results A Prompt or a Deferred alarm indicator lights on the following:

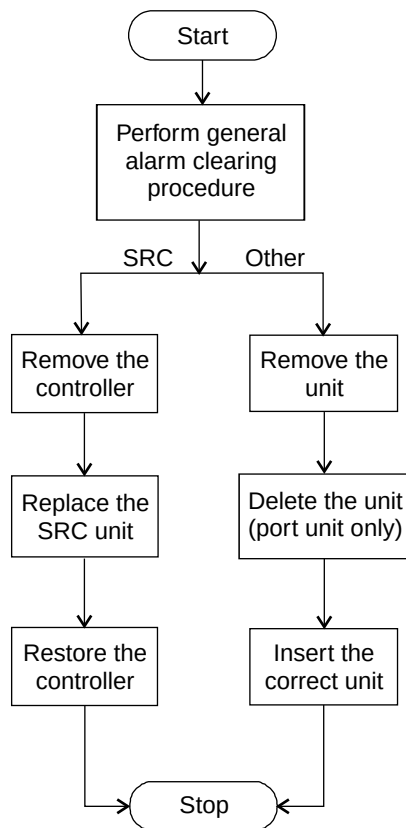
- User Panel
- End-of-suite
- Rack-top
- Station

The red LED on the affected unit is continuously lit.



WUPcEQ flowchart

Flowchart The following flowchart shows the procedure for clearing a WUPcEQ alarm.



□

Clearing WUPcEQ alarms for SRC units

Clearing actions **Important!** You will get a WUPcEQ alarm if an older version SRC unit was inserted into a subrack.

Use the following procedure to remove an older version SRC unit and to replace it with a unit of the correct version.

- 1 Perform the “General alarm clearing procedure” (21-8).
-

- 2 Put the SRC in the out-of-service state.

Reference: For more information, see one of the following topics:

- “Removing an MS subrack SRC from service” (11-33)
 - “Removing a port subrack SRC from service” (11-34)
-

- 3 Replace the unit.

Reference: For more information, see the following topics:

- “Removing a unit from the MS or port subrack” (2-11)
 - “Inserting a unit into the MS or port subrack” (2-13)
-

- 4 Restore the SRC.

Reference:

For more information, see “Restoring an SRC to service” (11-35).

END OF STEPS



Clearing WUPcEQ alarms for all units except SRC units

Clearing actions

Important! In most cases, the incorrect type of unit cannot be inserted into a slot because the backplane keys will prevent insertion.

If an incorrect type of unit that is keyed identically to the correct type of unit has been inserted into a particular slot, do the following:

- 1 Perform the “General alarm clearing procedure” (21-8).
- 2 Remove the unit.
- 3 Verify that the unit causing the alarm is the type of unit you want, and that the unit was not inserted in error.

If	Then
The alarmed unit is the <i>wrong</i> type of unit	Replace it with the correct type of unit and quit this procedure.
The alarmed unit is the <i>correct</i> type of unit	Go to Step 4.

- 4 Delete the port unit using the Unit window at *Provision > Equipment > Unit*. This will change the values back to the default data.
- 5 Reinsert the unit.

END OF STEPS





22 Product warranty and repair

Overview

Purpose This chapter describes the standard product warranty and how to return a product for repair.

Contents This chapter has the following topics:

- “Product warranty” (22-2)
- “Product repair guidelines” (22-4)
- “Procedure for returning defective equipment” (22-5)



Product warranty

Standard warranty The Standard Warranty supports new products. However, because Lucent Technologies may have two software releases available at one time, we are committed to warranty both the current product software release and one software release back. If the product does not fit these criteria, then the Standard Warranty does not apply.

The warranty period for a defective product repaired under warranty is 3 months, or the unexpired term of the new product warranty period, whichever is longer.

If Lucent Technologies does not install the product, the warranty term begins on the date the product is shipped. If Lucent Technologies installs the product, the warranty term begins when the installation is complete. All support services provided by Lucent Technologies will be provided by way of a separate Technical Support Contract which will be a component of the initial product sale. Beyond this warranty time frame, a separate extended-warranty contract must be agreed to by both Lucent Technologies and the customer at an additional and specified price.

The customer may make a warranty claim only if the customer has paid the full contracted price and has complied with all other obligations under this warranty agreement.

Hardware warranty *WaveStar*[™] DACS 4/4/1 hardware has a standard warranty period of 12 months. The product is warranted to be free from defects directly resulting from material and/or construction faults and conforms to the product's specifications referenced in Lucent Technologies documentation and as agreed to in the "Customer Purchase Agreement."

This warranty does not extend to damage resulting from natural wear and tear, incorrect, careless or incompetent treatment, exceeding environmental conditions (for example: air conditioning, humidity, etc.) by the customer, incorrect storage, or external causes such as fire or flooding.

Software warranty *WaveStar* DACS 4/4/1 software has a standard warranty period of 3 months. Lucent Technologies shall remedy to the best of its ability any malfunction free of charge, if the product software does not meet the functional specification. A warranty claim is possible only and so far as the customer demonstrates that the operational use of the product software essentially deviates from the functional specification.

No warranty is made that the product software will run uninterrupted or error-free. This warranty does not extend to damage resulting from

incorrect, careless or incompetent treatment by the customer, incorrect storage or external causes such as fire or flooding. Lucent Technologies also has the right to grant Right To Use (RTU) licenses for its software.

Discontinued availability

Lucent Technologies reserves the right to notify the customer in advance of the intention to Discontinue the Availability (DA) of a product. Lucent Technologies also reserves the right to offer a Technical Support Contract (TSC) to make repair and technical support services available for an additional period of time after a product has been discontinued. All TSC services will be at a specified price dependent on the terms and conditions of the contract.

The rights and obligations of Lucent Technologies and the customer shall neither be assigned nor delegated without prior written consent of the other party, except that Lucent Technologies may assign its obligations to any of its affiliates or non-Lucent Technologies contractors without further consent by the customer.

Warranty transfer

The entitlements of this warranty are not transferable.



Product repair guidelines

Standard repair If Lucent Technologies determines that a product is not defective or is in conformance, the customer shall pay Lucent Technologies the costs of handling, inspecting, testing, and transporting the product and, if applicable, travel and related expenses.

Repair interval Lucent Technologies repair locations set their own standards for return intervals. The minimum time to return a repaired product to the customer is 14 days from the receipt of the product by the repair location. The maximum time to return a repaired product to the customer can range from 50 to 180 days.

Out of warranty provisions For any activity associated with repair or replacement of hardware and/or software systems that is determined by Lucent Technologies to be out of warranty, materials and labour will be billed at Lucent Technologies list price (time-and-materials plus additional incurred expenses), or in accordance with the Technical Support Contract.



Procedure for returning defective equipment

Return address Return defective equipment with an Authorization To Repair Form to the following address:

Lucent Technologies
Charlotte Service Center
6701–A Northpark Blvd.
Charlotte, NC USA 28216
Attention: International Repair
Notify: Hipage Co. +1 704 357 3050

Procedure

- 1 Send a description of the defective equipment to the Lucent Technologies Charlotte Service Center. This should include the quantity, comcodes, and serial numbers (if available).

Result:

When the Charlotte Service Center receives the repair information, they will assign an order number and fax you an Authorization To Repair Form.

- 2 Send the Authorization To Repair form and the defective equipment to the Charlotte Service Center.
-

- 3 Fax the following information to the Charlotte Service Center:
 - Your return address
 - A customer contact name, telephone number, and fax number
 - Value of material
 - Identification of any hazardous equipment or material
 - Shipping information including the date of shipment, air waybill, carrier name, flight number, number of cartons, and weight of material

Result:

The Charlotte Service Center will send your equipment to a repair service. When the Charlotte Service Center receives the repaired equipment, they will ship you the repaired equipment, and fax you the shipping information.

.....

4 When you receive the repaired equipment, send the following information to the Charlotte Service Center:

- Order numbers for the equipment
- Date the equipment was received

Result:

When the Charlotte Service Center receives the order numbers and date, they will close the order.

END OF STEPS

.....





Glossary

A Abnormal alarm

An Abnormal alarm indicates that self tests, manual tests, or maintenance operations are in progress. The alarm is displayed via a yellow LED located on the User Panel. For example: a user manually switching the timing to holdover mode will cause an abnormal alarm. This feature is not yet available.

ACP

See Alarm Connector Panel.

Active

When an entity is duplicated, one of the duplicated entities (the active entity) is currently providing service, while the other is in standby. Either the working or protection entity could be active at any time.

Active and standby

These terms refer to the operational state of entities that are part of a protection group. An active entity is one that is currently providing service; a standby entity substitutes for an active entity if necessary.

A direction

The A direction is the direction in which the signal travels through the system from the E-END to the F-END, or the direction in a unidirectional cross connect.

Administrative Unit

An Administrative Unit (AU) is the information structure that provides adaptation between the higher order path layer and the Multiplex Section layer. The AU consists of a higher order Virtual Container information payload and an AU pointer. The AU pointer indicates the offset of the payload frame start relative to the Multiplex Section frame start. An AU-4 consists of a VC-4 plus an AU pointer. An AU-3 consists of a VC-3 plus an AU pointer.

Administrative Unit 3

An Administrative Unit 3 (AU-3) consists of a Virtual Container 3 (VC-3) plus an AU pointer.

Administrative Unit 4

An Administrative Unit 4 (AU-4) consists of a Virtual Container 4 (VC-4) plus an AU pointer.

Administrative Unit 4-4c

An Administrative Unit 4-4c (AU-4-4c) consists of four concatenated AU-4s. Concatenated means linked together in a series.

Administrative Unit Group

An Administrative Unit Group (AUG) consists of one or more byte-interleaved AUs. For an STM-1, an AUG can be either a single AU-4 or three byte-interleaved AU-3s.

AIS

See Alarm Indication Signal.

Alarm

An alarm is a visible or audible signal that indicates that an equipment failure or a significant event has occurred.

Alarm Connector Panel

The Alarm Connector Panel (ACP) is located on the back of the User Panel, below the Main Controller (MC) subrack. The ACP has connectors for alarm-related cables.

Alarm delay

Alarm delay is the amount of time the system waits after a failure occurs before activating an alarm.

Alarm Indication Signal

An Alarm Indication Signal (AIS) is a signal sent downstream indicating that an upstream failure has occurred. AIS is transmitted by the network element that detected the failure to prevent downstream failures being declared and alarms being raised.

Alarm indicator

An alarm indicator is a visual or audible indication that an alarm is active. One example of an alarm indicator is the red LED on a unit. The red LED lights if a unit fails.

Alarm Relay Unit

The Alarm Relay Unit (ARU) is located on the Main Controller (MC) subrack and provides system relay control and non 48V power distribution to the MC subrack.

Alarm severity

Alarm severity is an attribute that defines the priority of the alarm message. The way the system processes alarms depends on the alarm severity.

Alarm suppression

When you suppress an alarm, you selectively prevent the system from forwarding alarm messages to the user interface.

ALS

See Automatic Laser Shutdown.

American National Standards Institute

The American National Standards Institute (ANSI) is a standards-setting, non government organisation that develops and publishes standards for transmission codes, protocols, and high-level languages for voluntary use in the United States.

American National Standards Institute, Multiplex Section Protection

American National Standards Institute, Multiplex Section Protection (ANSI MSP) provides switching similar to unidirectional ITU MSP for STM-16, STM-4, and STM-1 optical interfaces, and for STM-1 electrical interfaces. ANSI MSP complies with American National Standards Institute (ANSI) T1–105.01. See International Telecommunications Union — Transmission, Multiplex Section Protection.

ANSI

See American National Standards Institute.

ANSI MSP

See American National Standards Institute, Multiplex Section Protection.

Apparatus code

Apparatus codes are unit codes used by the factory. For example, IM09 and LAH203 are apparatus codes.

ARU

See Alarm Relay Unit.

AU

See Administrative Unit.

AU-3

See Administrative Unit 3.

AU-4

See Administrative Unit 4.

AU-4-4c

See Administrative Unit 4_4c.

AUG

See Administrative Unit Group.

Automatic Laser Shutdown

Automatic Laser Shutdown (ALS) is a feature that causes the system to automatically shutdown the output power of laser transmitters and optical amplifiers. ALS can prevent a technician's eyes from being exposed to hazardous laser levels.

Auto-provisioning

Auto-provisioning is the system's ability to automatically provision equipment.

Autonomous

An autonomous command is initiated by the system without direction by a user.

Autonomous messages

Autonomous messages are messages generated automatically by the system.

B Background Block Errors

Background Block Errors (BBEs) are the number of errored blocks that were detected. A block is a set of consecutive bits associated with the path; each bit belongs to only one block. An Errored Block is a block in which one or more bits are in error.

Background test

An equipment diagnostic test is in background test mode when 2-6 diagnostic tests are running at the same time, and more than one unit is being tested. You can perform other tasks from the terminal while the system is executing tests in background mode.

Backup

Backup refers to the duplicate hardware, software, or data that can be used in case of failure, or when the primary system is unavailable.

Bandwidth

Bandwidth is the difference in Hz between the highest and lowest frequencies in a transmission channel. Bandwidth is also the data rate that can be carried by a given communications circuit.

BCC

See Board Controller Complex.

BCLAN

See Board Controller Local Area Network.

B direction

The B direction is the direction in which the signal travels through the system from the F-END to the E-END.

Bidirectional

Bidirectional, or two-way cross connects connect two ports so they can communicate in two directions.

Bit Slice Controller

The Bit Slice Controller (BSC) is located on the Matrix and Synchronisation (MS) subrack. The BSC works with the System Timing Unit (STU) to provide timing signals for internal transmission paths. The BSC also provides control information for the Bit Slice Switch Units (BSSUs). The BSC's interface module, the Optical Link Unit (OLU), provides the BSC's optical links to the switch matrix units, and to the BSC's duplicate mate. There are two OLUs for each BSC.

Bit Slice Fibre Interface

The Bit Slice Fibre Interface (BSFI) is a control interface between the Bit Slice Controller (BSC) and Bit Slice Switch Unit (BSSU). The Optical Link Unit (OLU) contains the circuitry for the BSFI. See also Equipment Core Interface.

Bit Slice Interface Unit

The Bit Slice Interface Units (BSIUs) are located on the port subracks. BSIUs transport data between the Bit Slice Switch Units (BSSUs) and the port units. The BSIU also monitors the transmission data and provides automatic protection switching for hardware failures.

Bit Slice Switch Unit

The Bit Slice Switch Units (BSSUs) are cross-connect matrix components. The WaveStar DACS has ten BSSUs. Five BSSUs are located in the bottom of the Matrix and Synchronisation rack, and five BSSUs are located in the bottom of the Matrix and Control rack. Each BSSU carries either 256 or 512 slices of Synchronous Digital Hierarchy (SDH) traffic (STM-1 equivalent).

Board Controller Complex

Many units contain Board Controller Complex (BCC) circuitry that allows the unit to talk to and be controlled by the Subrack Controller (SRC).

Board Controller Local Area Network

The Board Controller Local Area Network (BCLAN) is a subrack backplane communications link that the SRC uses to communicate with the other units in the subrack.

Boot

A boot transfers the contents of backup memory into working memory. Booting usually occurs when a unit or controller is inserted, when the system is powered up, or when a subrack is created.

Bridge cross connect

A bridge cross connect is another name for a multi-point cross connect.

Bridge (SNCP)

An SNCP bridge transmits identical traffic on both the working and protection trails.

Broadband

Broadband is a networking technique for transmitting large amounts of voice, data, image, and multimedia signals over long distances on coaxial or fibre-optic cables. In digital communication, signals are transmitted at the 45 Mbps or higher rate.

Broadcast cross connect

A broadcast cross connect is another name for a multi-point cross connect.

BSC

See Bit Slice Controller.

BSFI

See Bit Slice Fibre Interface.

BSIU

See Bit Slice Interface Unit.

BSSU

See Bit Slice Switch Unit.

C Central Office

A Central Office (CO) is a building that houses telecommunications equipment.

Circuit pack

See Unit.

CIT

See Craft Interface Terminal.

CO

See Central Office.

Cold start

A cold start initialises or recovers a single unit. A cold start may affect service.

Controller

Controller is another name for the Subrack Controllers (SRCs) and Main Processor Units (MPUs). Controllers administer the other units on their respective subracks.

Craft Interface Terminal

The Craft Interface Terminal (CIT) is a computer terminal used for provisioning and maintenance.

Cross connects

Cross connects are the hardware and software used to connect line-terminating equipment, multiplexers, and other equipment.

Current request

A current request is the current state of the entity with regard to protection switching. A current request is either the result of a previous user-initiated protection switch request or the result of a system-initiated switch request that was made due to the condition of the software and hardware. The current request is called the “current switch state” on the Integrated Transport Management-Subnetwork Controller (ITM-SC).

D DACS VI-2000

The Digital Access Cross-Connect System (DACS) VI-2000 was a first generation digital access cross-connect system with an initial capacity of 64 STM-1 equivalents.

DACScan

The DACScan was a network management system for a Data Communications Network (DCN). The DACScan is now called the Integrated Transport Management-Subnetwork Controller

(ITM-SC).

Default

A default is a value the system automatically provides if the user does not specify a value.

Defect

A defect is a fault that interrupts a specific function. A defect does not affect the performance of a function. See Failure.

Deferred

Deferred indicates one, or both, of the following:

- A change over to standby equipment has been used to restore service.
- A performance-degrading condition exists, but the condition does not affect service. Maintenance personnel must take immediate action, but they must resolve any prompt alarms first.

Degradation

Degradation pertains to the reduced service level available from a computer system when one or more of its component parts is unavailable due to malfunction or maintenance.

Diagnostic test

Tests the internal hardware on a unit.

Digital cross connect system

A digital cross connect is an electronic switching system that routes digital signals among multiple paths without the need to demultiplex signals.

Digital Timing Unit

The Digital Timing Unit (DTU) provides timing for the transmission units in a port subrack. The DTU is always duplicated.

Downstream

The downstream signal points at or towards the destination of the transmission stream. In other words, the downstream signal looks in the direction of transmission.

Drop and continue

A function within a ring node where traffic is both extracted from the working channels on the ring (drop), and transmitted onwards on the ring (continue).

DTU

See Digital Timing Unit.

Dual node interconnection

An architecture between two rings where two nodes in each ring are interconnected.

E ECI

See Equipment Core Interface.

E-END

E-END is an arbitrary designation used to distinguish one end of a unidirectional, bidirectional, idle (unmapped), or bridge cross connect as the signal travels through the system. You can establish test access at either the E-END or the F-END.

EID

See Equipment Identification.

Electrostatic Discharge

Electrostatic Discharge (ESD) is the sudden release of the charge associated with static electricity. Static charge is generated whenever two materials come into contact with each other and are then separated.

Entity

Entity is a term used to generically refer to a piece of equipment or to a signal.

Equipment Core Interface

The Equipment Core Interface (ECI) is a data and control interface between the Bit Slice Switch Unit (BSSU) and Bit Slice Interface Unit (BSIU). This interface also distributes the timing information between the port subracks and the BSSU. See Bit Slice Fibre Interface.

Equipment Identification

The Equipment Identification (EID) is the address the software uses to identify equipment.

Equipped

An equipped unit is a unit that has been successfully inserted into the subrack and has program image and configuration data.

Error

An error is any difference between a computed, observed, or measured condition and the theoretically-correct condition.

Errored

When a diagnostic test displays an errored message, it means that the system could not complete a diagnostic test.

Errored Seconds

Errored Seconds (ES) is a performance-monitoring parameter that refers to the number of one-second periods in which one or more Errored Blocks occur.

ESD

See Electrostatic Discharge.

Estimator value

The estimator value is a value that is used in the performance-monitoring calculation process. The estimator value is the error rate, in errored-blocks-per second, at which the errored seconds become severely-errored seconds.

ETSI

See European Telecommunications Standards Institute.

European Telecommunications Standards Institute

The European Telecommunications Standards Institute (ETSI) is a committee designed to provide inter-vendor and inter-operator compatibility of Synchronous Digital Hierarchy (SDH) equipment.

F F-END

F-END is an arbitrary designation used to distinguish the end opposite the E-END of a unidirectional, bidirectional, or bridge cross connect as the signal travels through the system. You can establish test access at either the E-END or the F-END.

Failed

When a diagnostic test displays a failed message, it means that the equipment did not pass a diagnostic test.

Failure

A failure is a defect that has persisted long enough to be considered a permanent condition. A failure can affect the performance of a specific function.

Far end

Far end refers to the *remote* network element. For performance monitoring, the system collects performance-monitoring data on the local network element from anomalies detected in the incoming signal by the remote (far-end) network element.

Fatal

A fatal condition means that the system has detected a fatal failure on either the active or the standby unit. A fatal failure is brought about by a unit being removed or by the loss of power to the unit.

Fibre-optic cable

Fibre-optic cable is a transmission medium consisting of a core of glass or plastic surrounded by a protective cladding, strengthening material, and outer jacket. Also called an optical-fibre cable.

Frame

A frame is the smallest repetitive block of digital data being transmitted.

Frame ID

The Frame ID uniquely identifies a system within the office.

Free-running mode

The system operates in free-running mode when it is initially put into service. In free-running mode, the system timing is provided by the internal clock. After the system has been phaselocked to a timing reference, the system will not return to free-running mode.

G G.xxx

G.xxx refers to ITU Standards documents.

Graphical User Interface

A Graphical User Interface (GUI) is a graphics-based user interface that incorporates icons, pull-down menus, and a mouse.

H Head end

A Sub-Network Connection Protection (SNCP) node that executes a bridge.

Hold off time

The time (0 to 10 seconds) that the system waits after detecting a failure before initiating a protection switch. The hold-off time can be used to control switching order when multiple protection mechanisms are protecting the same service. For example, lower order or higher order SNCP can be combined with MSP or equipment protection.

Holdover mode

Holdover mode is a backup operational mode that the system enters automatically if all provisioned timing references have failed. In holdover mode, the internal system clock simulates the timing that occurred during a previous period in free-running mode or phaselocked mode. An alarm is raised whenever the system enters holdover mode.

I Idle

An output port is idle if the port is not cross connected to an input port.

Information

An alarm designated as information means that the alarm requires no immediate action. Maintenance personnel can perform the required actions on a scheduled basis or after an accumulation of maintenance events. Information alarms are indicated only on the User Panel.

Initialisation

An initialisation is a restart that synchronises the hardware with the software. Warm and cold starts are also called initialisations.

Integrated Transport Management Network Module

An Integrated Transport Management Network Module (ITM-NM) is a network management system for a Data Communications Network (DCN). The ITM-NM was formerly called DACScan.

Integrated Transport Management Subnetwork Controller (ITM-SC)

The Integrated Transport Management Subnetwork Controller (ITM-SC) is the remote manager for Synchronous Digital Hierarchy (SDH) network elements in a subnetwork. The ITM-SC is also referred to as an Element Management System (EMS).

Interface Unit

The Interface Unit (IU) provides the SDH Physical Interface (SPI) function for STM-1 electrical and optical signals. All STM-1 IUs work with the STM-1 port unit.

International Telecommunications Union — Transmission

The International Telecommunications Union — Transmission (ITU) is an international consultative committee that studies technical, operating, and tariff questions and issues recommendations on them with a view to standardising telecommunications on a worldwide basis. The ITU was formerly called the Consultative Committee for International Telegraph and Telephone (CCITT).

International Telecommunications Union — Transmission, Multiplex Section Protection

International Telecommunications Union — Transmission, Multiplex Section Protection (ITU MSP) provides 1+1 unidirectional or bidirectional nonrevertive switching for STM-16, STM-4, and STM-1 optical interfaces, and for STM-1 electrical interfaces. Two lines carry identical payloads in a permanent bridged arrangement between network elements. ITU MSP complies with ITU-T Recommendation G.783, Annex A.

ITM-NM

See Integrated Transport Management Network Module.

ITM-SC

See Integrated Transport Management Subnetwork Controller.

ITU MSP

See International Telecommunications Union — Transmission, Multiplex Section Protection.

ITU-T

See International Telecommunications Union — Transmission.

IU

See Interface Unit.

K K bytes

K bytes are Automatic Protection Switching (APS) bytes that are used by the Multiplex Section Protection (MSP) functions at the ends of a multiplex section in making requests for, and giving acknowledgements of, protection-switching actions.

Kbps

The term Kbps refers to Kilobits per second.

L LAN hub

See Local Area Network hub.

LAN Hub Unit

The LAN Hub Units (LHUs) are located in the back of Main Controller subrack. The LHUs provide the hub ports for system LAN connections.

LHU

See LAN Hub Unit.

Line

Line refers to a transmission medium, together with the associated high speed equipment that are required for providing the means of transporting information between two consecutive network elements. One line originates the line signal, and the other line terminates the line signal.

Line condition

The line condition is the current state of health of a working or a protection line.

Line restore time

Line restore time is the number of minutes that the system waits, after a failure condition that caused a protection switch clears, before switching to the line that is not carrying service (the line where the fault cleared). Line restore time applies only to NTT MSP.

Line-derived timing

Line-derived timing means that the system timing is derived from the signal received from a transmission port.

Local Area Network hub

A Local Area Network (LAN) hub connects multiple LAN entities.

LOF

See Loss of Frame.

Loopback cross connect

A loopback cross connect is a special unidirectional cross connect that sends the signal from an input port back to the output port. Loopback cross connects are typically used to isolate trouble on the port units during installation.

Loopback test access connection

A loopback test access connection loops back one end of a signal onto itself and bridges the connection to the test access port. Use loopback test access connections to test idle ports. LOOPE and LOOPF are loopback test access connections.

LOP

See Loss of Pointer.

LOS

See Loss of Signal.

Loss of Frame

A Loss of Frame (LOF) is a failure to synchronise to an incoming signal.

Loss of Pointer

A Loss of Pointer (LOP) is a failure to extract good data from a signal payload.

Loss of Signal

A Loss of Signal (LOS) is the complete absence of an incoming signal.

M Magneto Optical disks

A Magneto Optical (MO) disk is a removable storage medium. MO disks are used for backing up the system database and for loading software onto the system.

Main Controller Local Area Network

The Main Controller Local Area Network (MCLAN) is a LAN used by the system for inter-processor communication between the Main Controller (MC) subrack and other system subracks.

Main Controller subrack

The Main Controller (MC) subrack contains the main processor, memory, Local Area Network (LAN) hubs, hard disk, removable optical disk, alarm unit, main connector panel, and User Panel.

Main Processor Unit

The Main Processor Unit (MPU) is located on the front of the Main Controller (MC) subrack. The MPU provides the central processing function which includes control of the ARU, LHU, and MSU.

Mass Storage Unit

The Mass Storage Unit (MSU) is located on the front of the Main Controller (MC) subrack. The MSU contains a hard disk drive and a Magneto-Optical (MO) drive.

Master unit

A master unit is a unit that controls a slave unit by sending messages or writing registers to the slave. BSC, DTU, and port units are master units.

Matrix and Control rack

The Matrix and Control (MC) rack is an equipment rack that contains the Main Controller subrack and five Bit Slice Switch Units (BSSUs).

Matrix and Synchronisation rack

The Matrix and Synchronisation (MS) rack is an equipment rack that contains the Matrix and Synchronisation subrack and five Bit Slice Switch Units (BSSUs).

Mbps

Mbps is a term that refers to Megabits per second. Mega is the Greek prefix for “big.” A megabit is one million bits.

MCLAN

See Main Controller Local Area Network.

Module

See Subrack.

Monitor test access connection

A monitor test access connection allows you to connect test equipment in parallel with a digital signal path while maintaining the digital transmission signal. Even though this test does *not* affect service, you will receive a confirmation notice from the user interface when you make a monitor test access connection. MONE, MONF, and MONEF are monitor test access connections.

MPU

See Main Processor Unit.

MS

See Multiplex section.

MSP

See Multiplex Section Protection.

MSU

See Mass Storage Unit.

Multiplexing

Multiplexing is the process of transmitting multiple signals over a single communications line or computer channel by interleaving the messages.

Multiplex section

A multiplex section (MS) is a transmission medium, together with the associated equipment, required to provide the means of transporting information between two consecutive network elements. One of the network elements originates the line signal and the other network element terminates the line signal.

Multiplex Section Protection

1+1 Multiplex Section Protection (MSP) is a transmission protection arrangement. The same signal is sent and received over two separate transmission lines. These transmission lines terminate on separate transmission ports that are logically linked in software. The system supports three types of MSP: ITU MSP, NTT MSP, and ANSI MSP.

Multiplex Section Protection group

A Multiplex Section Protection (MSP) group is a pair of associated ports on a pair of physically-adjacent port units. An MSP group, which is also called an MSP pair, provides transmission line protection between network elements.

Multiplex section terminating equipment

Multiplex section terminating equipment is a network element that originates or terminates STM-1, STM-4, or STM-16 signals.

Multi-point cross connect

Multi-point cross connects have the following characteristics:

- Connect a single input to two or more outputs
- Provide bridging for restoration, testing, or broadcast

- Can be from any input to any available output signal
- Created using the “Uni-Directional” option on the Cross Connect window
- Can be disconnected in any order
- Can be added to any existing service whether originally created as unidirectional or bidirectional
- Were previously called bridge and broadcast cross connects

N Near end

Near end refers to the *local* network element. For performance monitoring, the system collects performance-monitoring data on the local network element from anomalies detected in the incoming signal by the local (near-end) network element.

Network element

A network element is a piece of equipment that provides a component function in a network. Examples are: channel banks, digital cross-connects, and multiplexers.

Network Interface Chip

A Network Interface Chip (NIC) is a DEC 21140-A device capable of both 10BaseT or 100BaseT operations.

NIC

See Network Interface Chip.

Nippon Telephone and Telegraph, Multiplex Section Protection

Nippon Telephone and Telegraph, Multiplex Section Protection (NTT MSP) provides switching similar to bidirectional International Telecommunications Union, Multiplex Section Protection (ITU MSP) for STM-1 optical interfaces, and for STM-1 electrical interfaces. NTT MSP complies with ITU-T Recommendation G.783, Annex B, and a set of recommendations provided by NTT. See International Telecommunications Union — Transmission, Multiplex Section Protection.

Nonrevertive

Nonrevertive is a protection-switching operation type. When a protection group is nonrevertive, the protection entity will continue to operate as the active entity even after a failure clears on the working entity.

NTT MSP

See Nippon Telephone and Telegraph, Multiplex Section Protection.

O OLU

See Optical Link Unit.

Optical disk

An optical disk is a storage medium that contains digital data readable by optical techniques.

Optical Link Unit

The Optical Link Unit (OLU) is part of the internal transmission path. It provides interfaces for the optical-fibre cables that carry transmission data between the Bit Slice Controllers (BSCs) and the Bit Slice Switch Units (BSSUs). The OLU also provides interfaces for the optical-fibre cables that carry timing information between the duplicated BSCs in the Matrix and Synchronisation subrack.

OOS

See Out-of-service.

Optical-fibre cable

See Fibre-optic cable.

Out-of-service

Out-of-service is a controller state that means that the MPU and SRC controllers are in firmware mode. No application or system base is running.

Overhead

Overhead (OH) is the term for auxiliary bytes used for everything but customer payload (for example: signalling) carried with Synchronous Digital Hierarchy (SDH) signals.

P Pack

See Unit.

Parameter

Parameters are the output of the performance-monitoring calculation process. For example: background block errors, errored seconds, severely-errored seconds, and unavailable seconds are all parameters.

Partial Passed

When a diagnostic test displays a Partial Passed message, it means that the system tested and passed all the equipment *available* for the test in the current configuration. The screen will display this result if one or more units that could have been tested were not present, and therefore, were not tested.

Passed

When a diagnostic test displays a passed message, it means that the system tested all the equipment available for the test, and all of the equipment passed the diagnostic test.

Path terminating equipment

Path terminating equipment is a network element that multiplexes or demultiplexes the VC-4 payloads.

Path selector

Within an Sub-Network Connection Protection (SNCP) architecture, the node function that selects a tributary which is extracted from the working channels arriving from one side of the node or from the other side of the node, according to path level criteria.

Path Trace Identifier

The purpose of the Path Trace Identifier (PTI) is to transmit a path access point identifier so that a receiving terminal can verify that the receiving terminal is connected to the intended transmitter.

Performance monitoring

Performance monitoring (PM) measures the quality of service and identifies degrading or marginally operating systems before an alarm is generated.

Phaselocked mode

Phaselocked mode is the normal mode of operation. In this mode, the system clock is slaved to an external timing reference such as a transmission port or a station clock input.

Plug-in

See Unit.

PM

See Performance monitoring.

Port subrack

Port subrack is a generic term that refers to either the PSA or the PSC subracks.

Port subrack A

Port Subrack A (PSA) houses the STM-1 electrical and optical interfaces.

Port subrack C

Port Subrack C (PSC) houses the STM-4 or STM-16 optical interfaces.

Port unit

A port unit and an interface unit work together to transmit and receive optical or electrical signals. The STM-1, STM-4, and STM-16 units are port units.

Power Supply

The Power Supply (PSP) supplies DC power for the midplane, fans, and units in the Main Controller (MC) subrack. The PSP is located below the fan trays at the bottom of the MC subrack.

Power Terminal Module

The Power Terminal Module (PTM) filters incoming station power from two separate power sources and distributes power across the midplane.

Prompt

A prompt alarm indicates that maintenance personnel must repair the defective equipment or take whatever corrective action is necessary to restore good service. Alarms for conditions that affect service are always classified as prompt.

Protection

When an entity is duplicated, one of the duplicated entities is designated as the protection entity, while the other is designated as the working entity. If the status of the protection entity

changes from standby to active, the entity still retains its designation as the protection entity.

Protocol

Protocol is a formal set of conventions governing the format and relative timing of message exchange between two communicating processes.

Provisioning

Provisioning refers to the user's ability to create, change, view, and delete system information.

PSA subrack

See Port Subrack A.

PSC subrack

See Port Subrack C.

PSP

See Power Supply.

PTM

See Power Terminal Module.

R Rack

A rack is a mechanical assembly that houses the system equipment.

Revertive

Revertive is a protection-switching operation type. When a protection group is revertive, the system will automatically switch service from the protection entity back to the working entity when a failure clears and the Wait-To-Restore time has elapsed.

Rollover (Roll)

A roll is used to replace the input of an existing cross connect. All outputs specified in the original connection are moved to the new input. You can roll a unidirectional cross connect, one or both directions of a bidirectional cross connect, or a multi-point cross connection. When performing a roll, you can specify a specific output or all multi-point outputs.

S SCSI

See Small Computer System Interface.

SDH

See Synchronous Digital Hierarchy.

Secondary line (NTT MSP only)

The secondary line is the line in an NTT MSP arrangement that provides service when there is an active protection request.

Severely-Errored Seconds

Severely-Errored Seconds (SES) refers to the number of one-second periods in which the number of Errored Blocks equals or exceeds the estimator value.

Single node interconnection

An architecture between two rings where one node in each ring is interconnected.

Slave unit

A slave unit is a unit that is controlled by a master unit. BSSUs, BSIUs, and IUs are slave units.

Slot

A slot is the space in a subrack that is designed to hold a unit.

Small Computer System Interface

A Small Computer System Interface (SCSI) is a hardware interface that allows for the connection of peripheral devices to a computer.

SNCP

See Sub-Network Connection Protection.

Split test access connection

A split test access connection splits the digital transmission path so that you can perform tests in both directions. SPLTA, SPLTB, SPLTAB, SPLTE, SPLTF, and SPLTEF are split test access connections.

Squelch

A squelched signal means that no signal is being transmitted.

SRC

See Subrack Controller.

Standby

When an entity is duplicated, one of the duplicated entities, the active entity, is currently providing service while the other entity is in standby. Either the working or protection entity can be in standby at any time.

State

State indicates whether an entity is defective or normal, in service or out of service, etc.

Station alarm

A station alarm is an alarm that appears visually or audibly anywhere other than on the User Panel or on a unit.

Station clock input

The station clock input (2048 kHz or 64 kHz) depends on the type of System Timing Unit (STU) that is installed in the system.

STM

See Synchronous Transport Mode.

STU

See System Timing Unit.

Sub-Network Connection Protection

Sub-Network Connection Protection (SNCP) is a transmission protection feature that provides protection for all or part of a trail through a network. At the head end of the protected subnetwork connection, a bridge is created. The bridge sends two identical copies of the protected trail toward the tail end over different routes. The tail end selects which copy of the trail to take as input based on manual and automatic switching criteria. For bidirectional traffic, each end of the connection provides both the head end (bridging) and the tail end (selector) functions.

Subrack

A subrack is a mechanical assembly that houses plug-in units, also referred to as circuit packs, that contain the circuitry for the system. All subracks conform to European Telecommunications Standards Institute (ETSI) equipment practices for transmission products. Subracks have a midplane or a backplane that interconnects the units in the subrack.

Subrack Controller

The Subrack Controller (SRC) routes messages back and forth from the Main Controller (MC) to the units in the Matrix and Synchronisation subrack.

Suite

A suite is an equipment aisle or set of frames.

Synchronous

Synchronous is a method of transmitting data in which discrete signal elements are transmitted at a fixed and continuous rate. Synchronous data transmission requires that the timing of the transmission be synchronised between the sending and receiving devices.

Synchronous Digital Hierarchy

Synchronous Digital Hierarchy (SDH) is a hierarchical set of digital transport structures, standardised for the transport of suitably-adapted payloads over physical transmission networks.

Synchronous Transport Mode

The Synchronous Transport Mode (STM) is a transport and switching method that depends on information occurring in regular and fixed patterns with respect to a reference such as a frame pattern.

Synchronous Transport Module, level 1

Synchronous Transport Module, level 1 (STM-1) is a 155.52 Mbps data stream in a Synchronous Digital Hierarchy (SDH) frame format. This is the lowest level SDH signal.

Synchronous Transport Module, level n

Synchronous Transport Module, level “n” (STM-n) is a Synchronous Digital Hierarchy (SDH) standard for transmission over optical fibre by multiplexing “n” times the basic rate (STM-1).

- STM-4 = 622.08 Mbps
- STM-16 = 2.488 Mbps

System

System refers to groups of software and hardware that operate as a whole.

System clock input reference

System clock input references can be derived from transmission ports (STM-1, STM-4, STM-16 ports or MSP pairs) or from external timing references (station clock inputs). External references can be derived from one or two 2048 kHz timing inputs or from one or two 64 kHz composite clock inputs.

System Timing Unit

The System Timing Unit (STU) provides system timing and synchronisation. The STU-64 has an extra 64 KHz clock input for external timing purposes.

T Tail end

A Sub-Network Connection Protection (SNCP) node that requests the bridge.

TCA

See Threshold Crossing Alert.

Test access ports TP1 and TP2

Test access ports TP1 and TP2 are the software addresses for the test access ports. Test access ports are located on the port units.

Threshold

A threshold is the level of a parameter count at which the system sends a Threshold Crossing Alert.

Threshold Crossing Alert

The system reports a Threshold Crossing Alert (TCA) whenever a performance-monitoring parameter exceeds a specified threshold.

Trail

A trail is the logical transmission path between two path termination points.

Tributary Unit

A Tributary Unit (TU) is an information structure that provides adaptation between the lower order path layer and the higher order path layer. A TU consists of an information payload, also referred to as a lower order Virtual Container, and a TU pointer. The TU pointer indicates the offset of the payload frame start relative to the higher order Virtual Container frame start.

Tributary Unit 3

A Tributary Unit 3 (TU-3) consists of a Virtual Container 3 (VC-3) plus a TU pointer.

Tributary Unit 12

A Tributary Unit 12 (TU-12) consists of a Virtual Container 12 (VC-12) plus a TU pointer.

Tributary Unit Group

A Tributary Unit Group (TUG) consists of one or more TUs occupying fixed, defined positions in a higher order Virtual Container payload.

Tributary Unit Group 2

A TUG-2 is 12 columns of an STM-1 frame that can contain four TU-11s, three TU-12s, or one TU-2.

Tributary Unit Group 3

A TUG-3 is 86 columns of an STM-1 frame that can contain either one TU-3 or seven TUG-2s.

TU

See Tributary Unit.

TU-12

See Tributary Unit 12.

TU-3

See Tributary Unit 3.

TUG

See Tributary Unit Group.

TUG-2

See Tributary Unit Group 2.

TUG-3

See Tributary Unit Group 3.

U Unassigned alarm indicator

Unassigned alarms are customer-designed alarm interfaces. They consist of eight output relays for devices such as burglar alarms and fire detectors. Check office records for more details.

Unavailable Seconds

Unavailable Seconds is the number of one-second periods when performance-monitoring data is unavailable due to prolonged severely-errored conditions. The Unavailable Seconds count begins when the system detects ten or more consecutive Severely-Errored Seconds. The system will count these severely-errored seconds as an unavailable second instead. The Unavailable Seconds count stops when the system detects ten or more consecutive, nonseverely errored seconds. All other counts stop during Unavailable Seconds.

Unidirectional

A unidirectional, or one-way cross connect connects two ports so that they can communicate in one direction. Even though most cross connects are bidirectional, the system also allows cross connects in only one transmission direction between all port combinations. Unidirectional cross

connects are used mostly for test access.

Unit

A unit is the hardware that is inserted into an equipment shelf. A unit is also called a plug-in, circuit pack, or pack.

Upstream

The upstream signal points at or towards the source of the transmission stream. In other words, the upstream signal looks in the direction opposite to the direction of transmission.

V VC-4-4c

See Virtual Container 4_4c

VC

See Virtual Container.

VersaModule Europe

VersaModule Europe (VME) is a 1 through 21 slot, mechanical and electrical bus standard. VME is also known as the InterExchange Carrier (IEC) 821 bus.

Virtual Container

A Virtual Container (VC) is the information structure used to support path layer connections in the Synchronous Digital Hierarchy (SDH).

Virtual Container 4-4c

A Virtual Container 4-4c (VC-4-4c) consists of four concatenated VC-4s. Concatenated means linked together in a series.

VME

See VersaModule Europe.

W Wait-To-Restore time

The Wait-To-Restore (WTR) time is the amount of time (in minutes) that the system waits, after a failure condition that caused a protection switch clears, before switching back to the previously-active equipment (matrix slice or port unit).

Warm start

A warm start initialises or recovers a single unit or a group of units without affecting service.

Wideband

Wideband is one type of voice, data, or video rate that transmits digital rates between 1.5 Mbps and 45 Mbps.

Working

When an entity is duplicated, one of the duplicated entities is designated as the working entity, while the other is designated as the protection entity. If the status of the working entity changes from active to standby, the entity still retains its designation as the working entity. The working

entity is the preferred active entity.

WTR

See Wait-To-Restore time.



Index

Symbols

*K1 and *K2 mismatch
designations, [10-5](#)

Numerics

1+1 protection arrangement
description, [9-5](#)

1 by 8 protection
arrangement description,
[9-5](#)

2 by 8 protection
arrangement description,
[9-5](#)

10/100 BT connector on
the ARU, [2-17](#)

10/100 BASE T 1
connector on the NIC TM,
[2-25](#)

10/100 BASE T 2
connector on the NIC TM,
[2-26](#)

15 Minute field, [8-28](#)

24 Hour field, [8-28](#)

256 system capacity
addressing, [5-10](#)
information about, [1-5](#)

512 system capacity
addressing, [5-10](#)
information about, [1-5](#)

A ABNORMAL LED on User
Panel, [1-20](#)

ABT (Abort) switch on the
MPU, [2-21](#)

ACP, [1-22](#)

active entity description,
[9-5](#)

active units and diagnostic
tests, [12-12](#)

adapter for MD Input
diagnostic test

inserting, [12-51](#)

table of special
equipment, [12-13](#)

addresses

256 and 512 system
capacity, [5-10](#)

about entity, [5-2](#)

about physical layer,
[5-3](#)

about Signal ID, [5-4](#)

equipment protection
group, [5-16](#)

fibre, [5-19](#)

INTFcEQ, CABLEcEQ,
and CABLEcTIM
alarms, [5-19](#)

Main Controller, [5-11](#)

Matrix and
Synchronisation, [5-12](#)

MSP, [5-17](#)

PSA, [5-13](#)

PSC, [5-14](#)

rack top, [5-18](#)

wildcards, [5-9](#)

alarm clear delay timers,
[6-4](#)

alarm clearing

general flowchart, [21-7](#)

general procedure, [21-8](#)

list of alarms, [21-1](#)

on alarms caused by
diagnostic tests, [12-11](#)

order for clearing, [21-6](#)

Alarm Connector Panel,
[1-22](#)

ALARM I/O connector on
the ARU, [2-17](#)

Alarm Indicator ON Time
field, [13-6](#)

alarm indicator test

clearing a User Panel
failure, [13-15](#)

clearing an MC
end-of-suite test
failure, [13-11](#)

clearing an MC rack-top
failure, [13-13](#)

clearing an MS or port
subrack end-of-suite
test failure, [13-12](#)

- clearing an MS or port subrack rack-top test failure, [13-14](#)
- definitions, [13-3](#)
- procedure, [13-8](#)
- proving standby SRC can turn off alarm indicators, [13-10](#)
- Alarm Indicator Tests window
 - field descriptions, [13-6](#)
 - graphic of, [13-6](#)
- alarm indicators
 - definition, [6-8](#)
 - descriptions, [6-9](#)
 - information about disconnecting and suppressing, [6-12](#)
- Alarm Panel
 - displaying, [7-13](#)
 - information about, [6-5](#)
- Alarm Severity field, [7-3](#)
- alarm tallies, [6-5](#)
- Alarm Unit
 - See: ARU
- alarms
 - alarm and defect reports, [6-3](#)
 - alarm-clear delay timers, [6-4](#)
 - clearing alarms caused by diagnostic tests, [12-11](#)
 - conditions that affect service, [6-7](#)
 - consequent actions, [6-3](#)
 - correlating defects, [6-3](#)
 - defect-to-alarm delay timers, [6-4](#)
 - defects and failures, [6-3](#)
 - definitions, [6-2](#)
 - delay timers, types of, [6-4](#)
 - differences between transmission and equipment defects or failures, [6-3](#)
 - disconnecting, connecting, or suppressing station alarm indicators, [7-11](#)
 - displaying Alarm Panel, [7-13](#)
 - order for clearing, [21-6](#)
 - querying all, [7-4](#)
 - querying selected, [7-7](#)
 - querying station alarm indicator state (connected or disconnected), [7-10](#)
- alarms caused when a diagnostic test fails, [12-11](#)
- alarms caused when a diagnostic test passes, [12-11](#)
- Alarms menu, [4-10](#)
- alignment of PC and MC clocks, [4-3](#)
- All Autonomous Messages field, [8-10](#)
- All Data field, [8-27](#)
- All Defects field, [8-40](#)
- all files (*.*), [8-5](#)
- All Transactions field, [8-35](#)
- ALL, using in address, [5-9](#)
- ALM connector on the port rack fan tray connector panel, [1-32](#)
- ALM RMT connector on the ARU, [2-17](#)
- ALM/IO connector on the ARU, [2-17](#)
- Apply button, [4-17](#)
- architecture for protection switching, [9-5](#)
- arrows used for navigation, [4-20](#)
- ARU
 - clearing procedure for FLTcEQ alarm, [21-51](#)
 - general information about, [2-16](#)
 - in MC, [1-19](#)
- ARU ALARM 1 connector on the ACP, [1-23](#)
- ARU ALARM 2 connector on the ACP, [1-23](#)
- ARU ALT 1 connector on the ACP, [1-22](#)
- ARU ALT 2 connector on the ACP, [1-23](#)
- ARU RELAY 1 connector on the ACP, [1-22](#)
- ARU RELAY 2 connector on the ACP, [1-22](#)
- attenuators
 - DFTW optical STM-1 test with IM09 IUs, [12-31](#)
 - how to install, [12-28](#)
 - when to use, [12-13](#)
- AUcAIS alarm
 - clearing, [21-11](#)
 - description, [21-10](#)
- AUcLOP alarm
 - clearing, [21-14](#)
 - description, [21-13](#)
- AUI PORT 1 and AUI PORT 2 connectors on the NIC TM, [2-25](#)
- automatic laser
 - restart modes, [17-3](#)

- restarting, [17-5](#)
- automatic laser shutdown
 - information about, [17-2](#)
 - restarting, [17-5](#)
- Automatic Laser Shutdown window
 - field descriptions, [17-4](#)
 - graphic of, [17-4](#)
- autonomous events, [6-5](#)
- Autonomous Events button, [4-17](#)
- autonomous messages
 - querying all, [8-13](#)
 - querying by specifying a message type or entity, [8-15](#)
 - querying by specifying a time, [8-14](#)
 - querying the last message, [8-12](#)
- Autonomous Messages Query Results window
 - field descriptions for Alarms query, [8-18](#)
 - field descriptions for ALL query, [8-17](#)
 - field descriptions for Diagnostic Tests Completion Messages query, [8-19](#)
 - field descriptions for Port State Changes query, [8-24](#)
 - field descriptions for Protection Switch Events query, [8-20](#)
 - field descriptions for System Clock Reference Changes query, [8-21](#)
 - field descriptions for Threshold Crossing Alerts query, [8-22](#)

- field descriptions for Unit State Changes query, [8-23](#)
- graphic of, [8-16](#)
- Autonomous Messages window
 - field descriptions, [8-9](#)
 - graphic of, [8-9](#)

.....

B

- background mode, diagnostics, [12-8](#)
- Background Test field, [12-19](#)
- background tests
 - cancelling, [15-5](#)
 - displaying tests in progress, [15-4](#)
 - where to view, [15-2](#)
- Background Tests View Results window
 - field descriptions, [15-3](#)
 - graphic of, [15-3](#)
- backing up the database, [18-3](#)
- Backup Database window
 - graphic of, [18-2](#)
- backward compatible units, [2-31](#)
- battery power
 - clearing failure, [21-165](#)
 - information about, [21-163](#)
- BCLAN diagnostic test
 - clearing a failure, [12-26](#)
 - interpreting failure results, [12-23](#)
 - procedure and information about, [12-21](#)

- BCLANcEQ alarm
 - clearing, [21-17](#)
 - description, [21-16](#)
- Between field
 - Autonomous Messages window, [8-10](#)
 - Defects window, [8-40](#)
 - Performance Monitoring window, [8-27](#)
 - User Transactions window, [8-35](#)
- BFL LED on the MPU, [2-21](#)
- Bit Slice Controller
 - See: BSC
- Bit Slice Interface Unit
 - See: BSIU
- Bit Slice Switch Unit
 - See: BSSU
- block diagram
 - control system, [1-6](#)
 - system, [1-3](#)
- BNC cables
 - DFWT electrical diagnostic test, [12-45](#)
 - table of special equipment for diagnostic tests, [12-13](#)
- board controllers, [1-7](#)
- Board Failure LED on the MPU, [2-21](#)
- BOOTcSW alarm
 - clearing, [21-20](#)
 - description, [21-19](#)
- BOOTING state
 - SRC, [11-10](#)
 - Unit, [11-12](#)
- booting the PC, [4-2](#)

BOOT_FAIL state	BSSU to OLU cable connections	cable interfaces for
SRC, 11-9	See: Installation Assembly Manual	CABLEcEQ and CABLEcTIM alarms, 21-23
Unit, 11-12	BSSU Unit diagnostic test	INTFcEQ alarms, 21-110
Both 15 Minute and 24 Hour field, 8-28	clearing a failure, 12-84	cable tests, 12-16
BSC	running the test, 12-71	CABLEcEQ alarm
clearing procedure for FLTcEQ alarm, 21-53	button descriptions on Station Alarm Control window, 7-9	addresses, 21-23
flowchart for clearing a FLTcEQ alarm, 21-52	button test	clearing, 21-24
information about, 1-13	byte descriptions for the 64-byte field, 13-25	description, 21-22
BSC Unit diagnostic test	clearing a failure, 13-26	differences from CABLEcTIM, 21-28
clearing a failure, 12-84	procedure, 13-23	example of fibre address, 5-19
running the test, 12-68	Button Testing Test Results window	CABLEcTIM alarm
BSFI cable, 3-5	field descriptions, 13-24	addresses, 5-19
BSFI cable diagram	graphic of, 13-24	clearing, 21-29
See: Installation Assembly Manual	Button Tests window	description, 21-27
BSIU	field descriptions, 13-22	differences from CABLEcEQ, 21-28
clearing procedure for FLTcEQ alarm, 21-57	graphic of, 13-22	cables
flowchart for clearing a FLTcEQ alarm, 21-56	buttons, description of, 4-17	basic description of ECI and BSFI connections, 3-5
in PSA subrack, 1-29	byte descriptions	information about, 3-2
BSIU Unit diagnostic test	BCLAN diagnostic test, 12-23	inserting, 3-3
clearing a failure, 12-84	button test, 13-25	removing, 3-4
running the test, 12-71	DFWT electrical diagnostic test, 12-48	Cancel Test button, 4-17
BSIU128, 1-31	diagnostic tests, 12-91	cancelling background tests, 15-5
BSSU, 1-26		Category field
clearing procedure for FLTcEQ alarm, 21-57	C cable addresses, 5-19	Alarms query results from Autonomous Messages Query Results window, 8-18
flowchart for clearing a FLTcEQ alarm, 21-56	cable assignments	Defects query results, 8-44
information about, 1-15	querying, 19-4	View Current Alarms Query Results window, 7-5
BSSU Optical Loopback diagnostic test	table of, 19-3	
See: Optical Loopback diagnostic test	cable diagrams of BSFI and ECI	
	See: Installation Assembly Manual	

- Change button, [4-17](#)
- changing
 - alarm indicators, information about, [6-13](#)
- Checkstop LED on the MPU, [2-21](#)
- Checksum diagnostic test
 - clearing a failure, [12-84](#)
 - general information about, [12-3](#)
 - procedure and information about, [12-81](#)
- CHS LED on the MPU, [2-21](#)
- Clear AIS button, [4-17](#)
- Clear button, [4-17](#)
- Clear Forced Switch field
 - DTU window, [9-40](#)
 - Matrix Slice window, [9-20](#)
 - MS Control window, [9-10](#)
 - STM1 1:8 window, [9-51](#)
- Clear Freeze field
 - DTU window, [9-40](#)
 - Matrix Slice window, [9-20](#)
 - MS Control window, [9-9](#)
 - STM1 1:8 window, [9-51](#)
- Clear Lock Off field
 - Matrix Slice window, [9-21](#)
 - STM1 1:8 window, [9-52](#)
- Clear Lock On field
 - Matrix Slice window, [9-21](#)
 - STM1 1:8 window, [9-52](#)
- Clear Manual Switch field
 - DTU window, [9-41](#)
 - Matrix Slice window, [9-21](#)
 - MS Control window, [9-10](#)
 - STM1 1:8 window, [9-52](#)
- Clear Records button, [4-17](#)
- Clear status, [8-18](#)
- Clear Switch Request field
 - ITU and ANSI MSP, [10-26](#)
 - MSP transmission window (NTT), [10-27](#)
 - SNCP transmission window, [10-38](#)
- Clear Test History window
 - field descriptions, [16-2](#)
 - graphic of, [16-2](#)
 - clearing alarms
 - See: alarm clearing
 - clearing battery power failure, [21-165](#)
 - clearing protection states, [10-31](#), [10-42](#)
 - forced switches on DTU protection groups, [9-49](#)
 - forced switches on STM-1 1:8 protection groups, [9-60](#)
 - freezes on DTU protection groups, [9-49](#)
 - freezes on STM-1 1:8 protection groups, [9-60](#)
 - manual switches on DTU protection groups, [9-49](#)
 - matrix slice forced switch, [9-32](#)
 - matrix slice freeze, [9-30](#)
- matrix slice lock off, [9-36](#)
- matrix slice lock on, [9-38](#)
- matrix slice manual switch, [9-34](#)
- MS Control forced switch, [9-18](#)
- MS Control freeze, [9-18](#)
- clearing test records, [16-3](#)
- clock alignment, [4-3](#)
- Close button, [4-17](#)
- codes
 - error, [12-106](#)
 - failure, [12-103](#)
 - test, [12-93](#)
 - unit, [2-31](#)
- cold starts
 - difference between warm starts and, [11-5](#)
 - STU, BSC, BSSU, DTU, BSIU, and port units, [11-42](#)
 - when corresponding mate has a failure, [11-44](#)
- Command field
 - Background Tests View Results window, [15-3](#)
 - Diagnostic Tests Completion Messages query results, [8-19](#)
 - User Transactions Query Results window, [8-38](#)
- Command Parameters field, [8-38](#)
- Condition field
 - Alarms query results from Autonomous Messages Query Results window, [8-18](#)

- Defects query results, [8-43](#)
- conditions that affect service, [6-7](#)
- Connect button, [4-17](#)
- Connect Station Alarms button, [4-17](#)
- connecting
 - station alarm indicators, [7-11](#)
- connections to console terminal, [9-67](#)
- Connector panel, fan tray in port rack, [1-32](#)
- consequent actions, [6-3](#)
- console terminal, [9-67](#)
- CONSOLE/PORT 1
 - connector on the Serial TM, [2-28](#)
- control system, [1-6](#)
- Controller ID field, [11-17](#)
- controller maintenance
 - definitions, [11-4](#)
 - MPU out-of-service state, [11-6](#)
 - reason to remove SRC from service, [11-7](#)
 - tasks, [11-3](#)
- controller states, [11-9](#)
- controllers
 - information about subrack and board controllers, [1-6](#)
 - querying MPU, [11-16](#)
 - querying SRC, [11-16](#)
 - removing MPU in software on a duplicated MC, [11-18](#)
 - removing MPU in software on a single MC configuration, [11-22](#)
 - removing MS subrack SRC from service, [11-33](#)
 - removing port subrack SRC from service, [11-34](#)
 - restoring the database software on an MPU on a single MC, [11-29](#)
 - restoring the database software on an MPU with a duplicated MC, [11-23](#)
 - restoring to service, [11-35](#)
- copying information in a field, [4-20](#)
- correlating defects, [6-3](#)
- Count field, [8-31](#)
- CPU LED on the MPU, [2-21](#)
- Create button, [4-17](#)
- CRIT (critical) LED on the ARU, [2-16](#)
- cross-couple
 - communication link failure, [21-174](#)
- cross-couple timing link failure, [21-174](#)
- Current Alarms button, [4-17](#)
- Current Req field
 - DTU Query Results window, [9-43](#)
 - Matrix Slice Query Results window, [9-23](#)
 - MS Control Query Results window, [9-12](#)
- MSP transmission
 - Query Results window, [10-29](#)
- STM1 1:8 Query
 - Results window, [9-54](#)
- Current Req list of priorities
 - DTU Query Results window, [9-47](#)
 - ITU and ANSI MSP, [10-10](#)
 - Matrix Slice Query Results window, [9-27](#)
 - MS Control Query Results window, [9-16](#)
 - NTT MSP, [10-21](#)
 - STM1 1:8 Query Results window, [9-58](#)
- Current Req value descriptions
 - DTU Query Results window, [9-45](#)
 - ITU and ANSI MSP, [10-7](#)
 - Matrix Slice Query Results window, [9-25](#)
 - MS Control Query Results window, [9-14](#)
 - NTT MSP, [10-13](#)
 - STM1 1:8 Query Results window, [9-56](#)
- Current Request
 - SNCP list of priorities, [10-34](#)
 - SNCP value descriptions, [10-33](#)
- Current Request field
 - Protection Switch Events query results, [8-20](#)
 - SNCP transmission Query Results window, [10-40](#)

cutting information in a
field, [4-20](#)

D DACS

control system, [1-6](#)

functional description,
[1-3](#)

damage caused by
Electrostatic Discharge,
[2-4](#)

database

backup procedure, [18-3](#)

restoring on an MPU on
a single MC, [11-29](#)

restoring on an MPU
with a duplicated MC,
[11-23](#)

date and time
synchronisation warning,
[4-3](#)

Date Clear field, [8-18](#)

Date field, [15-3](#)

Diagnostic Tests
Completion Messages
query results, [8-19](#)

Performance Monitoring
Query Results window,
[8-30](#)

User Transactions Query
Results window, [8-38](#)

Date of Change field

Port State Changes
query results, [8-24](#)

Unit State Changes
query results, [8-23](#)

Date of Defect field, [8-43](#)

Date of Event field

ALL query results from
Autonomous Messages
Query Results window,
[8-17](#)

Protection Switch
Events query results,
[8-20](#)

System Clock Reference
Changes query results,
[8-21](#)

Date of Execution field,
[14-4](#)

Date of TCA field, [8-22](#)

Date Set field

Alarms query results
from Autonomous
Messages Query
Results window, [8-18](#)

View Current Alarms
Query Results window,
[7-5](#)

DBAVAIL state, [11-12](#)

DBOOS state, [11-10](#)

DCNcCAALOF alarm
clearing, [21-32](#)
description, [21-31](#)

DCNcMSNoNBR alarm
clearing, [21-35](#)
description, [21-34](#)

DCNcREPAIR alarm
clearing, [21-41](#)
description, [21-40](#)

DCNcRSNoNBR alarm
clearing, [21-38](#)
description, [21-37](#)

defect to alarm delay
timers, [6-4](#)

defective equipment, policy
for returning, [22-1](#)

defects

information about, [6-3](#)
querying, [8-42](#)

Defects Query Results
window
field descriptions, [8-43](#)

graphic of, [8-43](#)

Defects window

field descriptions, [8-40](#)
graphic of, [8-40](#)

DEFERRED LED on User
Panel, [1-20](#)

DEGcEQ alarm

clearing, [21-44](#)
description, [21-43](#)

delay timers, [6-4](#)

Delete button, [4-17](#)

Deleted Unit unit
condition, [9-59](#)

Description field

Button Testing Test
Results window, [13-24](#)
Diagnostic Testing Test
Results window, [12-88](#)

Designation field, [10-41](#)

Device EID field, [12-88](#)

Device ID field, [13-24](#)

DFWT electrical diagnostic
test

clearing a failure, [12-49](#)
how to interpret which
IU failed, [12-48](#)

procedure and
information about,
[12-44](#)

DFWT optical port unit
diagnostic test

clearing a failure, [12-42](#)
procedure and
information about
STM-1, [12-29](#)

- procedure and information about STM-16, [12-38](#)
- procedure and information about STM-4, [12-34](#)
- Diagnostic Testing Test Results window
 - field descriptions, [12-88](#)
 - graphic of, [12-88](#)
- diagnostic tests
 - alarms and LEDs caused by, [12-11](#)
 - byte descriptions for 64-byte field, [12-91](#)
 - cables, [12-16](#)
 - clearing a failure for Checksum, Disk Media, IIC, NVRAM, Register Test, Sanity Timer, or port Unit diagnostic tests, [12-84](#)
 - clearing alarms caused by, [12-11](#)
 - clearing BCLAN failures, [12-26](#)
 - clearing DFWT electrical failures, [12-49](#)
 - clearing DFWT optical port unit failures, [12-42](#)
 - clearing MCLAN failures, [12-86](#)
 - clearing MD Inputs failures, [12-54](#)
 - clearing Network Interface failures, [12-85](#)
 - clearing Optical Loopback failures, [12-60](#)
 - clearing Station Clock failures, [12-66](#)
- definitions, [12-6](#)
- description of, [12-3](#)
- error codes, [12-106](#)
- failure codes, [12-103](#)
- foreground and background modes, [12-8](#)
- how to interpret which IU failed the DFWT electrical test, [12-48](#)
- information about where to display results, [12-10](#)
- interpreting BCLAN failures, [12-23](#)
- procedure and information about Checksum, Disk Media, IIC, MCLAN, Network Interface, NVRAM, Register Test, Sanity Timer, and port Unit diagnostic tests, [12-81](#)
- protection state changes caused by, [12-12](#)
- protection switching caused by failed test, [12-12](#)
- removing units prior to and during, [12-15](#)
- running on active units, [12-12](#)
- running on more than one subrack, [12-14](#)
- special equipment for, [12-13](#)
- test codes, [12-93](#)
- units that must be standby, [12-12](#)
- what tests are available, [12-3](#)
- where to query results, [12-9](#)
- Diagnostic Tests window
 - field descriptions, [12-18](#)
 - graphic of, [12-18](#)
- Digital Timing Unit
 - See: DTU
- Disconnect button, [4-17](#)
- DISCONNECT Button Test field, [13-22](#)
- Disconnect Station Alarms button, [4-17](#)
- DISCONNECT switch on User Panel, [1-21](#)
- disconnectable station alarm indicators, [6-9](#)
- disconnecting
 - alarm indicators, information about, [6-12](#)
 - LOOPE test access mode, [20-62](#)
 - LOOPF test access mode, [20-66](#)
 - MONE test access mode, [20-9](#)
 - MONEF test access mode, [20-18](#)
 - MONF test access mode, [20-13](#)
 - SPLTA test access mode, [20-25](#)
 - SPLTAB test access mode, [20-41](#)
 - SPLTB test access mode, [20-32](#)
 - SPLTE test access mode, [20-47](#)
 - SPLTEF test access mode, [20-57](#)
 - SPLTF test access mode, [20-51](#)
- station alarm indicators, procedure, [7-11](#)

Disk Media diagnostic test	DTU	During the previous Hour(s) field
clearing a failure, 12-84	clearing procedure for FLTcEQ alarm, 21-61	Autonomous Messages window, 8-11
general information about, 12-4	flowchart for clearing a FLTcEQ alarm, 21-60	Defects window, 8-41
procedure and information about, 12-81	PSA subrack, 1-28	Performance Monitoring window, 8-28
DISKcFULL alarm	PSC, 1-30	User Transactions window, 8-36
clearing, 21-47	DTU protection switching	During the previous Minute(s) field
description, 21-46	querying, 9-42	Autonomous Messages window, 8-11
disks	requesting a protection switch, 9-49	Defects window, 8-41
See: MO disks	DTU query results, 9-43	Performance Monitoring window, 8-28
displaying	DTU Query Results window	User Transactions window, 8-36
Alarm Panel, 7-13	Current Req list of priorities, 9-47	
background tests in progress, 15-4	Current Req value descriptions, 9-45	E ECI cable description, 3-5
CABLEcEQ addresses, 21-23	field descriptions, 9-43	ECI cable diagram
diagnostic test result information, 12-10	graphic of, 9-43	See: Installation Assembly Manual
INTFcEQ addresses, 21-110	unit condition value descriptions, 9-48	Edit menu, 4-15
Do Not Revert	DTU Unit diagnostic test	editing with keys, 4-20
DTU Query Results window, 9-46	clearing a failure, 12-84	EIDs
MS Control Query Results window, 9-15	procedure and information about, 12-74	See: entity addresses
MSP transmission Query Results window (ITU and ANSI), 10-7	DTU window	Electrostatic Discharge, 2-4
MSP transmission Query Results window (NTT), 10-13	field descriptions, 9-40	Empty Slot unit condition
SNCP transmission Query Results window, 10-33	graphic of, 9-40	DTU Query Results window, 9-48
Do Not Revert Remote, 10-7	DUP cable problems, 21-90	MSP transmission Query Results (ITU and ANSI), 10-11
downward compatible units, 2-31	During the previous Day(s) field	MSP transmission Query Results (NTT), 10-23
	Autonomous Messages window, 8-11	STM1 1:8 Query Results window, 9-59
	Defects window, 8-41	End Day field, 8-27
	User Transactions window, 8-35	

End Time field	equipment defects or failures, 6-3	MONF test access mode, 20-12
Performance Monitoring Query Results window, 8-30	equipment diagnostic test terms, 12-6	SPLTA test access mode, 20-22
Performance Monitoring window, 8-27	equipment diagnostic tests See: diagnostic tests	SPLTAB test access mode, 20-36
end-of-suite alarm indicators, 6-9	equipment for diagnostic tests, 12-13	SPLTB test access mode, 20-29
end-of-suite indicator failure	Equipment ID field	SPLTE test access mode, 20-46
Main Controller, 13-11	Alarms query results from Autonomous Messages Query Results window, 8-18	SPLTEF test access mode, 20-54
Matrix and Synchronisation or port subrack, 13-12	Defects query results, 8-43	SPLTF test access mode, 20-50
entity addresses	View Current Alarms window, 7-5	Event Type field, 8-17
general information about, 5-2	equipment protection group addresses, 5-16	Execute button, 4-17
Main Controller, 5-11	equipment spares, list of, 2-32	Expected Fibre ID field, 19-5
Matrix and Synchronisation, 5-12	equipment terms, 1-11	external diagnostic tests, 12-13
PSA, 5-13	equipment, returning defective, 22-1	
PSC, 5-14	Equipped state	F FAIL LED on the port rack fan tray connector panel, 1-32
Signal ID, 5-4	SRC, 11-10	Failed field, 14-4
Entity ID field	Unit, 11-12	failure codes for diagnostic test results, 12-103
ALL query results from Autonomous Messages Query Results window, 8-17	error codes for diagnostic test results, 12-106	Failure Condition field
Performance Monitoring Query Results window, 8-30	Errored field, 14-4	View Current Alarms Query Results window, 7-6
Threshold Crossing Alerts query results, 8-22	ESD	failures, 6-3
View Results Query window, 14-4	See: Electrostatic Discharge	failures on diagnostic tests See: diagnostic tests
EOS 1 connector on the ACP, 1-23	establishing	Fan Connector Panel, 1-25
EOS 2 connector on the ACP, 1-23	LOOPE test access mode, 20-61	fan in MC subrack alarm clearing
EQPD state See: Equipped state	LOOPF test access mode, 20-65	clearing procedure for FLTcEQ alarm, 21-64
	MONE test access mode, 20-8	flowchart for clearing a FLTcEQ alarm, 21-63
	MONEF test access mode, 20-16	

- fan in port rack alarm clearing
 - flowchart for clearing an MDcIP alarm, [21-143](#)
- Fan tray connector panel in port rack, [1-32](#)
- Fatal, [9-17](#)
- FCP, [1-25](#)
- fibre addresses, [5-19](#)
- Fibre Assignments Query Results window
 - field descriptions, [19-5](#)
 - graphic of, [19-5](#)
- Fibre Assignments window
 - field descriptions, [19-2](#)
 - graphic of, [19-2](#)
- fibre connections, [3-5](#)
- fibre-optic cable assignments
 - addresses, [19-3](#)
 - querying, [19-4](#)
- fibre-optic cables
 - See: cables
- field descriptions
 - Alarm Indicator Tests window, [13-6](#)
 - Alarms query for Autonomous Messages Query Results window, [8-18](#)
 - ALL query for Autonomous Messages Query Results window, [8-17](#)
 - Automatic Laser Shutdown window, [17-4](#)
 - Autonomous Messages window, [8-9](#)
 - Background Tests View Results window, [15-3](#)
 - Button Testing Test Results window, [13-24](#)
 - Button Tests window, [13-22](#)
 - Clear Test History window, [16-2](#)
 - Defects Query Results window, [8-43](#)
 - Defects window, [8-40](#)
 - Diagnostic Testing Test Results window, [12-88](#)
 - Diagnostic Tests Completion Messages query for Autonomous Messages Query Results window, [8-19](#)
 - Diagnostic Tests window, [12-18](#)
 - DTU Query Results window, [9-43](#)
 - DTU window, [9-40](#)
 - Fibre Assignments Query Results window, [19-5](#)
 - Fibre Assignments window, [19-2](#)
 - LED Tests window, [13-17](#)
 - Login window, [4-4](#)
 - Matrix Slice Query Results window, [9-23](#)
 - Matrix Slice window, [9-20](#)
 - MC Control Query Results window, [9-64](#)
 - MS Control Query Results window, [9-12](#)
 - MS Control window, [9-9](#)
 - MSP transmission Query Results window, [10-29](#)
 - MSP transmission window for ITU and ANSI MSP, [10-25](#)
 - MSP transmission window for NTT MSP, [10-26](#)
 - Performance Monitoring Query Results window, [8-30](#)
 - Performance Monitoring window, [8-26](#)
 - Port State Changes query for Autonomous Messages Query Results window, [8-24](#)
 - Protection Switch Events query for Autonomous Messages Query Results window, [8-20](#)
 - SNCP protection window, [10-37](#)
 - SNCP transmission Query Results window, [10-40](#)
 - STM1 1:8 Query Results window, [9-54](#)
 - STM1 1:8 window, [9-51](#)
 - Subrack Control window, [11-15](#)
 - Subrack Controller Query Results window, [11-17](#)
 - System Clock Reference Changes query for Autonomous Messages Query Results window, [8-21](#)
 - Threshold Crossing Alerts query for Autonomous Messages Query Results window, [8-22](#)
 - Unit Control window, [11-38](#)

Unit State Changes
 query for Autonomous Messages Query
 Results window, [8-23](#)

User Transactions Query
 Results window, [8-38](#)

User Transactions
 window, [8-35](#)

View Current Alarms
 Query Results window, [7-5](#)

View Current Alarms
 window, [7-3](#)

View Results Query
 window, [14-4](#)

View Test Results
 window, [14-2](#)

fields, editing information
 in, [4-20](#)

File menu on application
 menu bar, [4-10](#)

File menu on query results
 menu bar, [4-14](#)

finding information in
 reports, [8-7](#)

FLOPPY/LED connector on
 the MPU, [2-22](#)

FLTcEQ alarm
 ARU, LHU, or PSP
 clearing procedure, [21-51](#)
 BSC or STU clearing
 procedure, [21-53](#)
 BSC or STU flowchart,
[21-52](#)
 BSIU or BSSU clearing
 procedure, [21-57](#)
 BSIU or BSSU
 flowchart, [21-56](#)
 description, [21-50](#)
 DTU clearing
 procedure, [21-61](#)
 DTU flowchart, [21-60](#)

fan in MC subrack
 alarm clearing
 procedure, [21-64](#)
 fan in MC subrack
 flowchart, [21-63](#)

IU or an unprotected
 port unit, clearing
 procedure, [21-67](#)

MPU clearing
 procedure, [21-69](#)

MSU clearing
 procedure, [21-70](#)

OLU clearing
 procedure, [21-72](#)

OLU flowchart, [21-71](#)

port unit that uses NTT
 MSP clearing
 procedure, [21-81](#)

port unit that uses NTT
 MSP flowchart, [21-80](#)

port unit that uses
 SNCP, ITU MSP, or
 ANSI MSP clearing
 procedure, [21-85](#)

port unit that uses
 SNCP, ITU MSP, or
 ANSI MSP flowchart,
[21-84](#)

SRC clearing flowchart,
[21-74](#)

SRC clearing procedure,
[21-75](#)

STM-1 electrical unit
 that uses 1:8
 protection clearing
 procedure, [21-77](#)

STM-1 electrical unit
 that uses 1:8
 protection flowchart,
[21-76](#)

FLTcSW alarm
 clearing for DUP cable
 problems, [21-90](#)

clearing on the MPU,
[21-91](#)
 clearing on the SRC,
[21-92](#)
 description, [21-89](#)

Force Reload field, [11-38](#)

Force Switch Slice {1-8}
 to Protect, [9-25](#)

Force Switch to Protect
 MSP transmission
 Query Results window
 (ITU and ANSI), [10-7](#)
 MSP transmission
 Query Results window
 (NTT), [10-13](#)
 SNCP transmission
 Query Results window,
[10-33](#)

Force Switch to Protect
 field
 DTU Query Results
 window, [9-45](#)
 DTU window, [9-40](#)
 Matrix Slice window,
[9-20](#)
 MS Control Query
 Results window, [9-14](#)
 MS Control window,
[9-9](#)
 MSP transmission
 window (ITU and
 ANSI), [10-25](#)
 MSP transmission
 window (NTT), [10-27](#)
 SNCP transmission
 window, [10-38](#)
 STM1 1:8 window, [9-51](#)

Force Switch to Protect
 Remote
 MSP transmission
 Query Results window
 (ITU and ANSI), [10-7](#)

MSP transmission Query Results window (NTT), 10-13	forcing protection states DTU protection groups to working or protection, 9-49	freezing protection states DTU protection groups, 9-49
Force Switch to Protect Request, 10-13	MS Control to working or protection, 9-18	matrix slice, 9-29
Force Switch to Working	MSP groups to working or protection, 10-31	MS Control, 9-18
MSP transmission Query Results window (ITU and ANSI), 10-7	SNCP transmission groups to working or protection, 10-42	STM-1 1:8 protection groups, 9-60
MSP transmission Query Results window (NTT), 10-13	STM-1 1:8 protection groups to working or protection, 9-60	functional description of system, 1-3
SNCP transmission Query Results window, 10-33	forcing to protection, 9-31	FUS (Fuse OK) LED on the MPU, 2-22
Force Switch to Working field	foreground mode, diagnostics, 12-8	fuse replacement, 21-165
DTU Query Results window, 9-45	Freeze field	
DTU window, 9-40	DTU Query Results window, 9-45	H Help, 4-23
MS Control Query Results window, 9-14	DTU window, 9-40	Help button, 4-18
MS Control window, 9-9	Matrix Slice Query Results window, 9-25	Help menu on application menu bar, 4-12
MSP transmission window (ITU and ANSI), 10-26	Matrix Slice window, 9-20	Help menu on query results menu bar, 4-15
MSP transmission window (NTT), 10-27	MS Control Query Results window, 9-14	Help Topics window, 4-23
SNCP transmission window, 10-38	MS Control window, 9-9	hierarchy of user interface, 4-8
Force Switch to Working Remote	SNCP transmission Query Results window, 10-33	HPcDEG alarm
MSP transmission Query Results window (ITU and ANSI), 10-7	SNCP transmission window, 10-37	clearing, 21-95
MSP transmission Query Results window (NTT), 10-13	STM1 1:8 Query Results window, 9-56	description, 21-94
Force Switch to Working Request, 10-13	STM1 1:8 window, 9-51	HPcPLM alarm
Force Switch Unit {1–8, 11–18} to Protect, 9-56	Freeze Slice {1–8} On Protect, 9-25	clearing, 21-98
	Freeze Unit {1–8, 11–18} on Protect, 9-56	description, 21-97
		HPcRDI alarm
		clearing, 21-101
		description, 21-100
		HPcTIM alarm
		clearing, 21-104
		description, 21-103
		HPcUNEQ alarm
		clearing, 21-107
		description, 21-106
		HTML file (*.html), 8-5

.....

I

icons, shortcut, [4-12](#)

IIC diagnostic test

- clearing a failure, [12-84](#)
- general information about, [12-4](#)
- procedure and information about, [12-81](#)

INFORMATION LED on User Panel, [1-20](#)

Initialisation Level field, [11-38](#)

Initialise button, [4-18](#)

initialising units

- cold starts on STU, BSC, BSSU, DTU, BSIU, and port units, [11-42](#)
- cold starts when corresponding mate has a failure, [11-44](#)
- SRC warm start, [11-40](#)
- warm starts on STU, BSC, DTU, and port units, [11-41](#)

Insert AIS button, [4-18](#)

inserting

- cables, [3-3](#)
- MO disks, [2-8](#)

inserting the MD Input Loopback Adapter, [12-51](#)

inserting the RF splitter, [12-63](#)

inserting units, [2-13](#)

installing attenuators, [12-28](#)

installing units

See: inserting units

Interface Unit

See: IU

interfaces for INTFcEQ alarms, [21-110](#)

interfaces, system, [1-8](#)

Interval field

Performance Monitoring Query Results window, [8-31](#)

Threshold Crossing Alerts query results, [8-22](#)

INTFcEQ alarm

addresses, [5-19](#)

addresses and interfaces, [21-110](#)

clearing, [21-111](#)

description, [21-109](#)

INVcCONF alarm

clearing, [21-114](#)

description, [21-113](#)

INVcDPLL alarm

clearing, [21-117](#)

description, [21-116](#)

INVcFPGA alarm

clearing on a BSC, DTU, or STU, [21-121](#)

clearing on port units, [21-123](#)

description, [21-120](#)

ITU and ANSI MSP

Current Req list of priorities, [10-10](#)

Current Req value descriptions, [10-7](#)

unit condition value descriptions, [10-11](#)

IU

clearing procedure for FLTcEQ alarm, [21-67](#)

in PSA subrack, [1-29](#)

IU field, [12-18](#)

IU Not Available unit condition, [9-59](#)

.....

K

K bytes, [10-5](#)

K1 and K2 mismatch state designations, [10-5](#)

KEYBOARD connector on the MPU, [2-22](#)

keys used for editing, navigating, and shortcuts, [4-20](#)

.....

L

LAH103 and LAH102 STU units and diagnostic tests, [12-62](#)

LAN Hub Unit

See: LHU

LAN PWR 1 LED on the NIC TM, [2-25](#)

LAN PWR 2 LED on the NIC TM, [2-25](#)

laser shutdown

information about, [17-2](#)

restarting, [17-5](#)

Last Autonomous Message field, [8-10](#)

LC/LC cables, [12-13](#)

LC/SC cables, [12-13](#)

LED ON Time field, [13-17](#)

LED test

clearing a unit LED failure, [13-19](#)

clearing a User Panel LED failure, [13-20](#)

procedure, [13-18](#)

LED Tests window

field descriptions, [13-17](#)

graphic of, [13-17](#)

LEDs	Locked & Operational unit condition	Lockout Force Switch Working Remote, 10-15
lit by diagnostic tests, 12-11	Matrix Slice Query Results window, 9-28	Lockout No Request, 10-15
on PTMs during tests, 13-4	STM1 1:8 Query Results window, 9-59	Lockout Remote, 10-7
on User Panel, 1-20	Locked & Slice Degrade, 9-28	Lockout Signal Degrade Protect, 10-15
LHU	Locked & Slice Fail, 9-28	Lockout Signal Degrade Protect Remote, 10-15
clearing procedure for FLTcEQ alarm, 21-51	Locked & Under Test unit condition, 9-59	Lockout Signal Degrade Working, 10-16
general information about, 2-18	Locked & Unit Fail unit condition, 9-59	Lockout Signal Degrade Working Remote, 10-16
MC subrack, 1-19	locking protection states	lockout switch request
Line Clear unit condition	MC, 9-71	MSP groups, 10-31
MSP transmission Query Results (ITU and ANSI), 10-11	STM-1 1:8 protection groups, 9-60	SNCP transmission groups, 10-42
MSP transmission Query Results (NTT), 10-23	locking service off of protection, 9-35	Lockout Trail Signal Fail Protect, 10-17
Line Restore Timer field, 10-29	locking service on to working	Lockout Trail Signal Fail Protect Remote, 10-17
link failure message, 4-2	matrix slice, 9-37	Lockout Trail Signal Fail Working, 10-16
Lock Service Off of Protect field	Lockout, 10-7	Lockout Trail Signal Fail Working Remote, 10-16
Matrix Slice Query Results window, 9-25	Lockout Do Not Revert, 10-14	Lockout Wait To Restore Protect, 10-17
Matrix Slice window, 9-21	Lockout field	Lockout Wait To Restore Protect Remote, 10-17
STM1 1:8 Query Results window, 9-56	ITU and ANSI MSP, 10-26	Lockout Wait To Restore Working, 10-18
STM1 1:8 window, 9-52	MSP transmission window (NTT), 10-27	Lockout Wait To Restore Working Remote, 10-18
Lock Service On to Working field	SNCP transmission Query Results window, 10-33	logging off the system, 4-6
Matrix Slice window, 9-21	SNCP transmission window, 10-38	logging on to the system, 4-4
STM1 1:8 window, 9-52	Lockout Force Switch Protect, 10-14	Login ID field
Locked & Empty Slot unit condition, 9-59	Lockout Force Switch Protect Remote, 10-14	Login window, 4-4
Locked & IU Not Available unit condition, 9-59	Lockout Force Switch Working, 10-14	Login window field descriptions, 4-4
		graphic of, 4-4

- Loop Count field
 - Background Tests View Results window, [15-3](#)
 - Diagnostic Tests Completion Messages query results, [8-19](#)
 - Diagnostic Tests window, [12-19](#)
 - looparound cables
 - DFWT electrical diagnostic test, [12-45](#)
 - DFWT optical STM-1 test with IM01 or IM05 IUs, [12-30](#)
 - DFWT optical STM-1 test with IM09 IUs, [12-31](#)
 - DFWT STM-16 diagnostic test, [12-39](#)
 - DFWT STM-4 diagnostic test, [12-35](#)
 - Optical Loopback diagnostic test, [12-57](#)
 - table of special equipment for diagnostic tests, [12-13](#)
 - LOOPE test access mode
 - disconnecting, [20-62](#)
 - establishing, [20-61](#)
 - information about, [20-60](#)
 - LOOPF test access mode
 - disconnecting, [20-66](#)
 - establishing, [20-65](#)
 - information about, [20-64](#)
 - LPcDEG alarm
 - clearing, [21-126](#)
 - description, [21-125](#)
 - LPcRDI alarm
 - clearing, [21-129](#)
 - description, [21-128](#)
 - LPcTIM alarm
 - clearing, [21-132](#)
 - description, [21-131](#)
 - LPcUNEQ alarm
 - clearing, [21-135](#)
 - description, [21-134](#)
-
- M**
- Magneto Optical disks
 - See: MO disks
 - main application window, [4-10](#)
 - Main Controller
 - clearing a rack-top test failure, [13-13](#)
 - clearing an end-of-suite test failure, [13-11](#)
 - entity addresses, [5-11](#)
 - information about control system, [1-6](#)
 - Main Controller field, [11-15](#)
 - Main Controller subrack, [1-17](#)
 - Main Processor Unit
 - See: MPU
 - Maintenance menu, [4-11](#)
 - MAJ (major) LED on the ARU, [2-16](#)
 - manual restart and restart for test of laser, [17-3](#)
 - Manual Restart button, [4-18](#)
 - Manual Restart for Test button, [4-18](#)
 - Manual Switch Slice {1-8} to Protect, [9-25](#)
 - Manual Switch to Protect
 - DTU window, [9-41](#)
 - MSP transmission
 - Query Results window (ITU and ANSI), [10-7](#)
 - SNCP transmission
 - Query Results window, [10-33](#)
 - Manual Switch to Protect field
 - DTU Query Results window, [9-46](#)
 - Matrix Slice window, [9-21](#)
 - MS Control Query Results window, [9-14](#)
 - MS Control window, [9-10](#)
 - MSP transmission window (ITU and ANSI), [10-25](#)
 - MSP transmission window (NTT), [10-27](#)
 - SNCP transmission window, [10-38](#)
 - STM1 1:8 window, [9-51](#)
 - Manual Switch to Protect Remote, [10-8](#)
 - Manual Switch to Working
 - DTU window, [9-41](#)
 - MSP transmission
 - Query Results window (ITU and ANSI), [10-8](#)
 - SNCP transmission
 - Query Results window, [10-33](#)
 - Manual Switch to Working field
 - DTU Query Results window, [9-46](#)
 - MS Control Query Results window, [9-15](#)
 - MS Control window, [9-10](#)

- MSP transmission window (ITU and ANSI), [10-26](#)
- MSP transmission window (NTT), [10-27](#)
- SNCP transmission window, [10-38](#)
- Manual Switch to Working Remote, [10-8](#)
- Manual Switch Unit {1–8, 11–18} to Protect, [9-57](#)
- manually restarting the laser, [17-5](#)
- manually switching protection states
 - DTU protection groups to working or protection, [9-49](#)
 - MS Control to working or protection, [9-18](#)
 - MSP groups to working or protection, [10-31](#)
 - SNCP groups to working or protection, [10-42](#)
 - STM-1 1:8 protection groups to working or protection, [9-60](#)
- manually switching to protection, [9-33](#)
- Mass Storage Unit
 - See: MSU
- master units, [11-8](#)
- Matrix and Control rack description, [1-16](#)
- Matrix and Synchronisation
 - clearing a rack-top test failure, [13-14](#)
 - clearing an end-of-suite test failure, [13-12](#)
 - entity addresses, [5-12](#)
 - inserting units into subrack, [2-13](#)
 - removing units from subrack, [2-11](#)
- Matrix and Synchronisation rack, [1-12](#)
- Matrix and Synchronisation subrack, [1-13](#)
- matrix slice protection switching
 - clearing a forced switch, [9-32](#)
 - clearing a freeze, [9-30](#)
 - clearing a lock off, [9-36](#)
 - clearing a lock on, [9-38](#)
 - clearing manual switch, [9-34](#)
 - forcing to protection, [9-31](#)
 - freezing protection states, [9-29](#)
 - locking service off protection, [9-35](#)
 - locking service on to working, [9-37](#)
 - manually switching to protection, [9-33](#)
 - querying, [9-22](#)
- Matrix Slice query results, [9-23](#)
- Matrix Slice Query Results window
 - Current Req list of priorities, [9-27](#)
 - Current Req value descriptions, [9-25](#)
 - field descriptions, [9-23](#)
 - graphic of, [9-23](#)
 - unit condition value descriptions, [9-28](#)
- Matrix Slice window
 - field descriptions, [9-20](#)
 - graphic of, [9-20](#)
- MC and PC clock alignment, [4-3](#)
- MC Control query results, [9-64](#)
- MC Control Query Results window
 - field descriptions, [9-64](#)
 - graphic of, [9-64](#)
- MC Duplication Functions screen, [9-68](#)
- MC protection switching, [9-71](#)
 - querying from console terminal, [9-70](#)
 - querying from user interface, [9-63](#)
- MC subrack
 - See: Main Controller
- MCLAN diagnostic test
 - clearing a failure, [12-86](#)
 - general information about, [12-4](#)
 - procedure and information about, [12-81](#)
- MCLANcEQ alarm
 - clearing, [21-139](#)
 - description, [21-137](#)
 - flowchart, [21-138](#)
- MD IN connector on the FCP, [1-25](#)
- MD Input Loopback Adapter
 - inserting, [12-51](#)
 - table of special equipment for diagnostic tests, [12-13](#)
- MD inputs and outputs, [6-10](#)
- MD Inputs diagnostic test
 - clearing a failure, [12-54](#)

- procedure and information about, [12-51](#)
- MD OUT connector on the FCP, [1-25](#)
- MDcIP alarm
 - description, [21-142](#)
 - fan in port rack flowchart, [21-143](#)
- MDcIP alarm on a fan in a port rack
 - clearing, [21-144](#)
- MDI 1 through 4 connectors on the FCP, [1-25](#)
- MDIs and MDOs, [6-10](#)
- Member ID field
 - DTU Query Results window, [9-43](#)
 - Matrix Slice Query Results window, [9-23](#)
 - MC Control Query Results window, [9-64](#)
 - MS Control Query Results window, [9-12](#)
 - MSP transmission Query Results window, [10-29](#)
 - STM1 1:8 Query Results window, [9-54](#)
- menu bar
 - on main application window, [4-10](#)
 - on query results windows, [4-14](#)
- Message/Event Type field, [8-10](#)
- messages, general
 - information about, [4-22](#)
- MINR (minor) LED on the ARU, [2-16](#)
- MISC DISCRETES
 - connector on the ACP, [1-24](#)
- miscellaneous discrete alarm
 - connectors, [21-142](#)
 - indicators, [6-10](#)
- Miscellaneous Discrete Inputs diagnostic test, [12-4](#)
- MO disks
 - capacity, [2-7](#)
 - general information about, [2-7](#)
 - inserting, [2-8](#)
 - removing, [2-9](#)
- MONE test access mode
 - disconnecting, [20-9](#)
 - establishing, [20-8](#)
 - information about, [20-7](#)
- MONEF test access mode
 - disconnecting, [20-18](#)
 - establishing, [20-16](#)
 - information about, [20-15](#)
- MONF test access mode
 - disconnecting, [20-13](#)
 - establishing, [20-12](#)
 - information about, [20-11](#)
- Monitoring Control... button
 - general information about, [4-18](#)
- MOUSE connector on the MPU, [2-22](#)
- MPU
 - clearing procedure for FLTcEQ alarm, [21-69](#)
- general information about, [2-21](#)
- in MC subrack, [1-18](#)
- out-of-service state, [11-6](#)
- querying, [11-16](#)
- reason to remove from service, [11-6](#)
- removing from service in the software on a duplicated MC, [11-18](#)
- removing from service in the software on a single MC configuration, [11-22](#)
- restoring the database software on a duplicated MC, [11-23](#)
- restoring the database software on a single MC, [11-29](#)
- MS Control protection switching
 - querying, [9-11](#)
 - requesting a protection switch, [9-18](#)
- MS Control query results, [9-12](#)
- MS Control Query Results window
 - Current Req list of priorities, [9-16](#)
 - Current Req value descriptions, [9-14](#)
 - field descriptions, [9-12](#)
 - graphic of, [9-12](#)
 - unit condition value descriptions, [9-17](#)
- MS Control window
 - field descriptions, [9-9](#)
 - graphic of, [9-9](#)

MScAIS alarm - clearing, 21-148 - description, 21-147 MScDEG alarm - clearing, 21-151 - description, 21-150 MScFOP alarm - clearing, 21-154 - description, 21-153 MScRDI alarm - clearing, 21-157 - description, 21-156 MSP addresses, 5-17 MSP groups - ITU and ANSI Current Req value descriptions, 10-7 - NTT Current Req value descriptions, 10-13 - querying, 10-28 - requesting a protection switch, 10-31 MSP ID field, 10-29 MSP transmission Query Results window - field descriptions, 10-29 - graphic of, 10-29 MSP transmission window - graphic of, 10-25 - ITU and ANSI MSP field descriptions, 10-25 - NTT MSP field descriptions, 10-26 MSP unit condition value descriptions - ITU and ANSI, 10-11 - NTT, 10-23	MSU - clearing procedure for FLTcEQ alarm, 21-70 - general information about, 2-23 - in MC subrack, 1-18 N NARROW SCSI connector on the ARU, 2-17 navigating with keys, 4-20 Network Element field, 4-4 Network Interface Chip TM, 1-19 Network Interface diagnostic test - clearing a failure, 12-85 - general information about, 12-4 - procedure and information about, 12-81 network interfaces, 1-8 New Monitoring State field, 8-24 New Reference ID field, 8-21 New Reference Number field, 8-21 New State field, 8-23 NIC TM, 2-25 No Request - MSP transmission Query Results window (ITU and ANSI), 10-8 - MSP transmission Query Results window (NTT), 10-18 - SNCP transmission Query Results window, 10-33	No Request field - DTU Query Results window, 9-46 - Matrix Slice Query Results window, 9-26 - MS Control Query Results window, 9-15 - STM1 1:8 Query Results window, 9-57 nondisconnectable station alarm indicators, 6-9 NTT MSP - Current Req list of priorities, 10-21 - Current Req value descriptions, 10-13 - unit condition value descriptions, 10-23 NVRAM diagnostic test - clearing a failure, 12-84 - general information about, 12-4 - procedure and information about, 12-81 O OAM and P interfaces, 1-8 Old Reference ID field, 8-21 Old Reference Number field, 8-21 Old State field, 8-23 OLU - clearing procedure for FLTcEQ alarm, 21-72 - flowchart for clearing a FLTcEQ alarm, 21-71 - in Matrix and Synchronisation subrack, 1-14

OLU to BSSU cable connections See: Installation Assembly Manual		PORT 4 connector on the Serial TM, 2-29
OOScSW alarm clearing, 21-160 description, 21-159	P Parameter field, 8-31 Parameters field, 8-17 Partial Pass field, 14-4 Passed field, 14-4 Password field, 4-4 pasting information in a field, 4-20 PC and MC clock alignment, 4-3 PC booting, 4-2 PC connected to name, displaying, 4-7 PC for user interface, 4-2 PC information, 4-2 PCI LED on the MPU, 2-22 PCI MEZZANINE CARD on the MPU, 2-22 performance monitoring date and time report discrepancies, 8-33 Performance Monitoring Query Results window field descriptions, 8-30 graphic of, 8-30 Performance Monitoring window field descriptions, 8-26 graphic of, 8-26 performance monitoring, querying data, 8-29 physical layer addresses, 5-3 PM Parameter field, 8-22 PORT 2 connector on the Serial TM, 2-28 PORT 3 connector on the Serial TM, 2-29	Port ID field Fibre Assignments Query Results window, 19-5 Fibre Assignments window, 19-2 Port ID, information about, 5-3 port rack, description and illustration, 1-27 port subracks clearing a rack-top test failure, 13-14 clearing an end-of-suite test failure, 13-12 inserting units into, 2-13 PSA, 1-28 PSC, 1-30 removing units from, 2-11 POWcDEG alarm clearing, 21-164 description, 21-162 POWER LED on User Panel, 1-20 Power Supply See: PSP Power Terminal Modules See: PTMs precautions against Electrostatic Discharge, 2-4 Primary ID field SNCP transmission window, 10-37 Print button, 4-18 printing reports, 8-6
Operational unit condition DTU Query Results window, 9-48 Matrix Slice Query Results window, 9-28 MS Control Query Results window, 9-17 SNCP transmission Query Results, 10-35 STM1 1:8 Query Results window, 9-59		
Operations, Administration, Maintenance, and Provisioning interfaces, 1-8		
optical fibre cable addresses, 5-19		
Optical Link Unit See: OLU		
Optical Loopback diagnostic test clearing a failure, 12-60 procedure and information about, 12-56		
optical-fibre cables See: cables		
order for clearing alarms, 21-6		
out-of-service state MPU, 11-6 SRC, 11-7		

- priorities for protection switching, [9-7](#)
- priorities, Current Req list
 - ITU and ANSI MSP, [10-10](#)
 - NTT MSP, [10-21](#)
- priorities, SNCP Current Request list, [10-34](#)
- product warranty and repair, [22-1](#)
- PROMPT LED on User Panel, [1-20](#)
- Protect Slice field, [9-21](#)
- protection entity description, [9-5](#)
- Protection Group ID field, [8-20](#)
- Protection menu, [4-11](#)
- Protection Not Available, [9-56](#)
- protection state changes caused by diagnostic tests, [12-12](#)
- Protection Switch Control button
 - Diagnostic Tests window, [12-19](#)
 - general information about, [4-18](#)
- Protection Switch Transmission Query Results
 - See: MSP transmission Query Results
- protection switching information
 - architecture, [9-5](#)
 - choosing the correct window, [9-3](#)
 - definitions for equipment, [9-4](#)
 - definitions for Main Controller, [9-66](#)
 - differences between active and standby, [9-5](#)
 - differences between working and protection, [9-5](#)
 - failed diagnostic tests and, [12-12](#)
 - MSP and SNCP switch request definitions, [10-3](#)
 - operation types, [9-6](#)
 - priorities, [9-7](#)
 - protection arrangements, [9-5](#)
- protection switching procedures
 - clearing a forced switch on the matrix slice, [9-32](#)
 - clearing a freeze of the matrix slice, [9-30](#)
 - clearing a manual switch on the matrix slice, [9-34](#)
 - clearing a matrix slice lock off, [9-36](#)
 - clearing a matrix slice lock on, [9-38](#)
 - DTU protection group switch requests, [9-49](#)
 - forcing the matrix slice to protection, [9-31](#)
 - freezing the matrix slice, [9-29](#)
 - locking the matrix slice off protection, [9-35](#)
 - locking the matrix slice on to working, [9-37](#)
 - manually switching the matrix slice to protection, [9-33](#)
 - MC switch requests, [9-71](#)
- MS Control switch requests, [9-18](#)
- MSP group switch requests, [10-31](#)
- querying DTU protection groups, [9-42](#)
- querying MC from console terminal, [9-70](#)
- querying MC from user interface, [9-63](#)
- querying MS Control, [9-11](#)
- querying MSP groups, [10-28](#)
- querying SNCP group switch status, [10-39](#)
- querying STM-1 1:8 protection groups, [9-53](#)
- querying the matrix slice protection state, [9-22](#)
- SNCP transmission group switch requests, [10-42](#)
- STM-1 1:8 protection group switch requests, [9-60](#)
- Provision menu, [4-10](#)
- PSA entity addresses, [5-13](#)
- PSA port subrack, [1-28](#)
- PSC entity addresses, [5-14](#)
- PSC port subrack, [1-30](#)
- PSP
 - clearing procedure for FLTcEQ alarm, [21-51](#)
 - general information about, [2-19](#)
- PTMs
 - during tests, [13-4](#)
 - in Matrix and Synchronisation subrack, [1-14](#)

in PSA subrack, [1-29](#)
in PSC subrack, [1-31](#)
PWR connector on the port
rack fan tray connector
panel, [1-32](#)

fibre-optic cable
assignments, [19-4](#)
matrix slice protection
state, [9-22](#)
MC protection
switching from console
terminal, [9-70](#)
MC protection
switching from user
interface, [9-63](#)
MPU controller, [11-16](#)
MS Control protection
switching, [9-11](#)
MSP groups for
switching, [10-28](#)
performance-monitoring
data, [8-29](#)
SNCP group switch
status, [10-39](#)
SRC, [11-16](#)
station alarm indicator
state (connected or
disconnected), [7-10](#)
STM-1 1:8 protection
groups, [9-53](#)
User transactions, [8-37](#)

Matrix and
Synchronisation
description and
illustration, [1-12](#)
port rack description
and illustration, [1-27](#)
Received Fibre ID field,
[19-5](#)
recommended spare
equipment, [2-32](#)
record update procedure,
[4-16](#)
record updates, [4-15](#)
records, general
information about queries,
[4-14](#)
recovering from Wrong
unit in slot state, [11-36](#)
Register Test diagnostic
test
clearing a failure, [12-84](#)
general information
about, [12-5](#)
procedure and
information about,
[12-81](#)
Remove button, [4-19](#)
removing
cables, [3-4](#)
MO disks, [2-9](#)
MPU from service in
the software on a
duplicated MC, [11-18](#)
MPU from service in
the software on a
single MC
configuration, [11-22](#)
SRC from service,
reason for, [11-7](#)
removing SRC from
service in the software
MS subrack SRC, [11-33](#)

Q Query Active button, [4-18](#)
Query All Login IDs field,
[8-35](#)
Query button, [4-18](#)
Query From ID button,
[4-18](#)
Query NE Date/Time
button, [4-18](#)
Query PC Date/Time
button, [4-18](#)
Query Port button, [4-18](#)
query results, general
description of, [4-14](#)
Query Specific Login ID
field, [8-35](#)
Query Standby button, [4-18](#)
Query To ID button, [4-18](#)
querying
alarms, all, [7-4](#)
alarms, selected, [7-7](#)
autonomous messages,
all messages, [8-13](#)
autonomous messages,
by specifying a
message type or entity,
[8-15](#)
autonomous messages,
by specifying a time,
[8-14](#)
autonomous messages,
last message, [8-12](#)
defects, [8-42](#)
diagnostic tests, [12-9](#)
DTU protection groups,
[9-42](#)

R RACK TOP 1 connector on
the ACP, [1-23](#)
RACK TOP 2 connector on
the ACP, [1-23](#)
rack top addresses, [5-18](#)
rack-top alarm indicators,
[6-9](#)
rack-top indicator failure
Main Controller, [13-13](#)
Matrix and
Synchronisation or
port subrack, [13-14](#)
racks
Matrix and Control
description, [1-16](#)

- port subrack SRC, [11-34](#)
- removing units
 - before and during diagnostic tests, [12-15](#)
 - in Matrix and Synchronisation or port subrack, [2-11](#)
- repair guidelines, [22-1](#)
- replacement procedure for FLTcEQ alarm
 - ARU, LHU, or PSP, [21-51](#)
 - BSC or STU, [21-53](#)
 - BSIU or BSSU, [21-57](#)
 - DTU, [21-61](#)
 - fan in MC subrack, [21-64](#)
 - IU or an unprotected port unit, [21-67](#)
 - MPU, [21-69](#)
 - MSU, [21-70](#)
 - OLU, [21-72](#)
 - port unit that uses NTT MSP, [21-81](#)
 - port unit that uses SNCP, ITU MSP, or ANSI MSP, [21-85](#)
 - SRC, [21-75](#)
 - STM-1 electrical unit that uses 1:8 protection, [21-77](#)
- replacing blown fuse, [21-165](#)
- reports
 - date and time discrepancies, [8-33](#)
 - finding information in, [8-7](#)
 - information about, [8-3](#)
 - printing, [8-6](#)

- querying all autonomous message, [8-13](#)
- querying autonomous messages by specifying a message type or entity, [8-15](#)
- querying autonomous messages by specifying a time, [8-14](#)
- querying defects, [8-42](#)
- querying performance-monitoring data, [8-29](#)
- querying the last autonomous message, [8-12](#)
- querying user transactions, [8-37](#)
- saving to a file, [8-5](#)
- Reports menu, [4-11](#)
- requesting a protection switch
 - choosing the correct window, [9-3](#)
 - DTU protection group, [9-49](#)
 - MC, [9-71](#)
 - MS Control, [9-18](#)
 - MSP groups, [10-31](#)
 - SNCP transmission groups, [10-42](#)
 - STM-1 1:8 protection groups, [9-60](#)
- Reset switch on the MPU, [2-21](#)
- restarting the laser
 - information about, [17-3](#)
 - procedure, [17-5](#)
- Restore All button, [4-19](#)
- Restore button, [4-19](#)

- restoring
 - database software on an MPU on a single MC, [11-29](#)
 - database software on an MPU with a duplicated MC, [11-23](#)
 - SRC to service in the software, [11-35](#)
- Result field
 - Button Testing - Test Results window, [13-24](#)
 - Diagnostic Testing - Test Results window, [12-88](#)
 - Diagnostic Tests Completion Messages query results, [8-19](#)
- Result Type field, [14-2](#)
- RF splitter
 - inserting for diagnostic tests, [12-63](#)
 - table of special equipment for diagnostic tests, [12-13](#)
- Roll button, [4-19](#)
- RScLOF alarm
 - clearing, [21-168](#)
 - description, [21-167](#)
- RST switch on the MPU, [2-21](#)

.....

S SA Status field

- Alarms query results from Autonomous Messages Query Results window, [8-18](#)
- Defects query results, [8-44](#)
- Sanity Timer diagnostic test
 - clearing a failure, [12-84](#)

- general information about, [12-5](#)
- procedure and information about, [12-81](#)
- Save Error Message button, [4-19](#)
- saving reports to a file, [8-5](#)
- SC/LC cables, [12-13](#)
- SC/SC cables, [12-13](#)
- screens
 - See: windows
- SCSI IN connector on the SCSI TM, [2-27](#)
- SCSI OUT connector on the SCSI TM, [2-27](#)
- SCSI TM
 - general information about, [2-27](#)
 - in MC, [1-19](#)
- sequence for clearing alarms, [21-6](#)
- Serial Number field
 - View Results Query window, [14-4](#)
 - View Test Results window, [14-2](#)
- Serial TM
 - general information about, [2-28](#)
 - in MC, [1-19](#)
- Service Affecting field, [7-6](#)
- service-affecting conditions, [6-7](#)
- Set NE Date/Time button, [4-19](#)
- Set PC Date/Time button, [4-19](#)
- Set status, [8-18](#)
- setting up the RF splitter, [12-63](#)
- Severity field
 - Alarms query results from Autonomous Messages Query Results window, [8-18](#)
 - Defects query results, [8-43](#)
 - View Current Alarms Query Results window, [7-6](#)
- shortcut keys, [4-20](#)
- shortcuts to user interface windows, [4-12](#)
- shutting down the laser, [17-2](#)
- Side Fail, [9-17](#)
- Signal Degrade Protect
 - MSP transmission Query Results window (ITU and ANSI), [10-8](#)
 - MSP transmission Query Results window (NTT), [10-18](#)
- Signal Degrade Protect Remote
 - MSP transmission Query Results window (ITU and ANSI), [10-8](#)
 - MSP transmission Query Results window (NTT), [10-18](#)
- Signal Degrade Protect Request, [10-18](#)
- Signal Degrade unit condition
 - MSP transmission Query Results (ITU and ANSI), [10-11](#)
 - MSP transmission Query Results (NTT), [10-23](#)
- Signal Degrade Working
 - MSP transmission Query Results window (ITU and ANSI), [10-8](#)
 - MSP transmission Query Results window (NTT), [10-19](#)
- Signal Degrade Working Remote
 - MSP transmission Query Results window (ITU and ANSI), [10-8](#)
 - MSP transmission Query Results window (NTT), [10-19](#)
- Signal Degrade Working Request, [10-19](#)
- Signal ID field
 - general information about, [5-4](#)
 - graphical representation of wideband signal, [5-8](#)
 - table of signal layer addresses, [5-4](#)
- signal layer addresses, [5-4](#)
- signal type and entity ID combinations for specifying multiplexing, [5-4](#)
- Signal Type field
 - SNCP transmission window, [10-37](#)
- slave units, [11-8](#)
- Slice Degrade, [9-28](#)
- Slice Fail, [9-28](#)
- Slice {1-10} Degrade, [9-25](#)
- Slice {1-10} Fail, [9-25](#)
- SNCP Current Request
 - list of priorities, [10-34](#)
 - value descriptions, [10-33](#)

- SNCP groups
 - Current Request value descriptions, [10-33](#)
 - querying switch status, [10-39](#)
 - requesting a protection switch, [10-42](#)
 - unit condition descriptions, [10-35](#)
- SNCP transmission Query Results window
 - field descriptions, [10-40](#)
 - graphic of, [10-40](#)
- SNCP transmission window
 - field descriptions, [10-37](#)
 - graphic of, [10-37](#)
- socket failure message, [4-2](#)
- sorting query records, [4-14](#)
- spare equipment, list of, [2-32](#)
- splitter
 - inserting for diagnostic tests, [12-63](#)
 - table of special equipment for diagnostic tests, [12-13](#)
- SPLTA test access mode
 - disconnecting, [20-25](#)
 - establishing, [20-22](#)
 - information about, [20-21](#)
- SPLTAB test access mode
 - disconnecting, [20-41](#)
 - establishing, [20-36](#)
 - information about, [20-35](#)
- SPLTB test access mode
 - disconnecting, [20-32](#)
 - establishing, [20-29](#)
- information about, [20-28](#)
- SPLTE test access mode
 - disconnecting, [20-47](#)
 - establishing, [20-46](#)
 - information about, [20-45](#)
- SPLTEF test access mode
 - disconnecting, [20-57](#)
 - establishing, [20-54](#)
 - information about, [20-53](#)
- SPLTF test access mode
 - disconnecting, [20-51](#)
 - establishing, [20-50](#)
 - information about, [20-49](#)
- SRC
 - clearing procedure for FLTcEQ alarm, [21-75](#)
 - controller states, [11-9](#)
 - flowchart for clearing a FLTcEQ alarm, [21-74](#)
 - in Matrix and Synchronisation subrack, [1-13](#)
 - in PSA subrack, [1-28](#)
 - in PSC subrack, [1-30](#)
 - initialising, [11-40](#)
 - out-of-service state, [11-7](#)
 - querying controller, [11-16](#)
 - reason to remove from service, [11-7](#)
 - removing MS subrack SRC from service, [11-33](#)
 - removing port subrack SRC from service, [11-34](#)
 - restoring to service, [11-35](#)
- SRC ID field, [11-15](#)
- standby entity description, [9-5](#)
- standby units and diagnostic tests, [12-12](#)
- Start Day field, [8-27](#)
- Start Time field
 - Performance Monitoring Query Results window, [8-30](#)
 - Performance Monitoring window, [8-27](#)
- State field, [11-17](#)
- states
 - SRC, [11-9](#)
 - unit, [11-11](#)
- STATION ALARM
 - connector on the ACP, [1-23](#)
- Station Alarm Control window
 - button descriptions, [7-9](#)
 - graphic of, [7-9](#)
- station alarm indicator state queries, [7-10](#)
- station alarm indicators
 - disconnecting, connecting, or suppressing, [7-11](#)
 - information about, [6-9](#)
- Station Clock diagnostic test
 - clearing a failure, [12-66](#)
 - procedure and information, [12-62](#)

Status field	STM-1 Unit diagnostic test	Current Req value descriptions, 9-56
Alarms query results from Autonomous Messages Query Results window, 8-18	clearing a failure, 12-84	field descriptions, 9-54
Performance Monitoring Query Results window, 8-31	procedure and information about, 12-81	graphic of, 9-54
STM-1	STM-16, 1-30	unit condition value descriptions, 9-59
clearing procedure for FLTcEQ alarm on an electrical unit that uses 1:8 protection, 21-77	STM-16 unit	STM1 1:8 window
flowchart for clearing a FLTcEQ alarm for an electrical unit that uses 1:8 protection, 21-76	flowchart for clearing a FLTcEQ alarm on unit that uses NTT MSP, 21-80	field descriptions, 9-51
in PSA subrack, 1-28	flowchart for clearing a FLTcEQ alarm on unit that uses SNCP, ITU MSP, or ANSI MSP, 21-84	graphic of, 9-51
STM-1 1:8 protection groups	STM-16 Unit diagnostic test	STMcLOS alarm
querying, 9-53	clearing a failure, 12-84	clearing, 21-171
requesting a protection switch, 9-60	procedure and information about, 12-81	description, 21-170
STM-1 unit	STM-4, 1-30	storing MO disks, 2-7
clearing procedure for FLTcEQ alarm on an unprotected unit, 21-67	STM-4 unit	structure of user interface, 4-8
clearing procedure for FLTcEQ alarm on unit that uses NTT MSP, 21-81	flowchart for clearing a FLTcEQ alarm on unit that uses NTT MSP, 21-80	STU
clearing procedure for FLTcEQ alarm on unit that uses SNCP, ITU MSP, or ANSI MSP, 21-85	flowchart for clearing a FLTcEQ alarm on unit that uses SNCP, ITU MSP, or ANSI MSP, 21-84	clearing procedure for FLTcEQ alarm, 21-53
flowchart for clearing a FLTcEQ alarm on unit that uses NTT MSP, 21-80	STM-4 Unit diagnostic test	flowchart for clearing a FLTcEQ alarm, 21-52
flowchart for clearing a FLTcEQ alarm on unit that uses SNCP, ITU MSP, or ANSI MSP, 21-84	clearing a failure, 12-84	in Matrix and Synchronisation subrack, 1-13
	procedure and information about, 12-81	STU Station Clock diagnostic test
	STM1 1:8 query results, 9-54	See: Station Clock diagnostic test
	STM1 1:8 Query Results window	STU Unit diagnostic test
	Current Req list of priorities, 9-58	clearing a failure, 12-84
		procedure and information about, 12-77
		STU Unit field, 8-21
		STUs, type to run diagnostic tests, 12-62
		subrack control tasks, 11-3
		Subrack Control window
		field descriptions, 11-15
		graphic of, 11-15

Subrack Controller See: SRC	Switching Mode field	system capacity, displaying, 1-5
Subrack Controller field, 11-15	SNCP transmission Query Results window, 10-40	System Controller LED on the MPU, 2-22
Subrack Controller Query Results window field descriptions, 11-17 graphic of, 11-17	Switching Type field MSP transmission Query Results window, 10-29	system description, 1-3 system interfaces, 1-8 system messages, general information about, 4-22 system name, displaying, 4-7
subrack controllers, 1-6	SYNCCCRF alarm clearing, 21-176 description, 21-173 flowchart, 21-175 possible causes, 21-174	
Subrack Degrade Inhibit button, 4-19	SYNCCLTRF alarm clearing, 21-182 description, 21-179 flowchart, 21-180	T tabbed text (*.txt), 8-5 TCP/IP, 1-8 TEMPcEQ alarm clearing, 21-203 description, 21-202
subracks Main Controller description and illustrations, 1-17 Matrix and Synchronisation description and illustrations, 1-13 PSA port subrack description and illustrations, 1-28 PSC port subrack description and illustrations, 1-30	SYNCCROOR alarm clearing, 21-186 description, 21-185 SYNCCSCF alarm clearing, 21-189 description, 21-188 SYNCCSCHO alarm clearing, 21-192 description, 21-191 SYNCCSTCOF alarm clearing, 21-196 description, 21-194 flowchart, 21-195 SYNCCSTCRF alarm clearing, 21-200 description, 21-199	terminal connections, 9-67 test access conventions used in, 20-5 definitions, 20-4 what is needed to begin, 20-3 test codes for diagnostic test results, 12-93 Test Executed field, 14-4 Test field Alarm Indicator Tests window, 13-6 Background Tests View Results window, 15-3 Clear Test History window, 16-2 Diagnostic Tests Completion Messages query results, 8-19 Diagnostic Tests window, 12-18 View Test Results window, 14-2
subracks with tests running on more than one subrack, 12-14	synchronisation and timing capabilities, 1-9	
SUPPRESS Button Test field, 13-22	SYS LED on the MPU, 2-22 system capacities, 1-5	
Suppress Station Alarms button, 7-9		
SUPPRESSED switch on User Panel, 1-21		
suppressing alarm indicators, information about, 6-12 station alarm indicators, procedure, 7-11		

- Test LED on the ARU, [2-16](#)
- Test Name field
 - Button Testing - Test Results window, [13-24](#)
 - Diagnostic Testing - Test Results window, [12-88](#)
- test records, clearing, [16-3](#)
- Test Results for the Device field, [12-89](#)
- test results, viewing, [14-3](#)
- Test Type field
 - Alarm Indicator Tests window, [13-6](#)
 - Background Tests View Results window, [15-3](#)
 - Diagnostic Tests Completion Messages query results, [8-19](#)
 - Diagnostic Tests window, [12-18](#)
- tests
 - See: diagnostic tests
- Threshold field, [8-22](#)
- Time Clear field, [8-18](#)
- Time field, [15-3](#)
 - Diagnostic Tests Completion Messages query results, [8-19](#)
 - User Transactions Query Results window, [8-38](#)
- Time of Change field
 - Port State Changes query results, [8-24](#)
 - Unit State Changes query results, [8-23](#)
- Time of Defect field, [8-43](#)
- Time of Event field
 - ALL query results from Autonomous Messages Query Results window, [8-17](#)
 - Protection Switch Events query results, [8-20](#)
 - System Clock Reference Changes query results, [8-21](#)
- Time of Execution field, [14-4](#)
- Time of TCA field, [8-22](#)
- time out messages, [4-22](#)
- Time Set field
 - Alarms query results from Autonomous Messages Query Results window, [8-18](#)
 - View Current Alarms window, [7-5](#)
- time zones and performance monitoring data, [8-33](#)
- toolbar
 - Help Topics window, [4-23](#)
 - Main Application window, [4-12](#)
- trail of lights, [6-8](#)
- Trail Signal Degrade Protection, [10-33](#)
- Trail Signal Degrade unit condition, [10-35](#)
- Trail Signal Degrade Working, [10-33](#)
- Trail Signal Fail Protect
 - MSP transmission Query Results window (ITU and ANSI), [10-8](#)
- MSP transmission
 - Query Results window (NTT), [10-19](#)
- SNCP transmission
 - Query Results window, [10-33](#)
- Trail Signal Fail Protect Remote
 - MSP transmission Query Results window (ITU and ANSI), [10-8](#)
- MSP transmission
 - Query Results window (NTT), [10-19](#)
- Trail Signal Fail Protect Request, [10-19](#)
- Trail Signal Fail unit condition
 - MSP transmission Query Results (ITU and ANSI), [10-11](#)
- MSP transmission
 - Query Results (NTT), [10-23](#)
- SNCP transmission
 - Query Results, [10-35](#)
- Trail Signal Fail Working
 - MSP transmission Query Results window (ITU and ANSI), [10-9](#)
- MSP transmission
 - Query Results window (NTT), [10-19](#)
- SNCP transmission
 - Query Results window, [10-33](#)
- Trail Signal Fail Working Remote
 - MSP transmission Query Results window (ITU and ANSI), [10-9](#)
- MSP transmission
 - Query Results window (NTT), [10-20](#)

Trail Signal Fail Working Request, [10-20](#)

Trail Type field

- Performance Monitoring Query Results window, [8-30](#)
- Threshold Crossing Alerts query results, [8-22](#)

Transition Module, [1-19](#)

transmission defects or failures, [6-3](#)

Transmission Protected unit condition, [9-59](#)

TST LED on the ARU, [2-16](#)

TST-MODE switch on the ARU, [2-16](#)

TUcAIS alarm

- clearing, [21-206](#)
- description, [21-205](#)

TUcLOM alarm

- clearing, [21-209](#)
- description, [21-208](#)

TUcLOP alarm

- clearing, [21-212](#)
- description, [21-211](#)

U Under Test unit condition

- DTU Query Results window, [9-48](#)
- STM1 1:8 Query Results window, [9-59](#)

UNEQPD

See: Unequipped

UNEQPD state

See: Unequipped state

Unequipped state

- SRC, [11-10](#)
- Unit, [11-12](#)

UNicEQ alarm

- clearing for most cases, [21-215](#)
- clearing when alarm appears after SRC insertion, [21-216](#)
- clearing when alarm is raised against a BSSU, [21-217](#)
- description, [21-214](#)

unit condition descriptions for SNCP, [10-35](#)

Unit Condition field

- DTU Query Results window, [9-43](#)
- Matrix Slice Query Results window, [9-24](#)
- MS Control Query Results window, [9-12](#)
- MSP transmission Query Results window, [10-30](#)
- SNCP transmission Query Results window, [10-41](#)
- STM1 1:8 Query Results window, [9-55](#)

unit condition value descriptions

- DTU Query Results window, [9-48](#)
- ITU and ANSI MSP, [10-11](#)
- Matrix Slice Query Results window, [9-28](#)
- MS Control Query Results window, [9-17](#)
- NTT MSP, [10-23](#)
- STM1 1:8 Query Results window, [9-59](#)

unit control tasks, [11-3](#)

Unit Control window

- field descriptions, [11-38](#)
- graphic of, [11-38](#)

Unit diagnostic test

- BSC procedure and information, [12-68](#)
- BSIU and BSSU procedure and information, [12-71](#)
- clearing a failure, [12-84](#)
- DTU procedure and information, [12-74](#)
- port unit procedure and information, [12-81](#)
- STU procedure and information, [12-77](#)

Unit Fail Protect

- DTU Query Results window, [9-45](#)
- MS Control Query Results window, [9-14](#)

Unit Fail unit condition

- DTU Query Results window, [9-48](#)
- MSP transmission Query Results (ITU and ANSI), [10-11](#)
- MSP transmission Query Results (NTT), [10-23](#)
- STM1 1:8 Query Results window, [9-59](#)

Unit Fail Working

- DTU Query Results window, [9-45](#)
- MS Control Query Results window, [9-14](#)

Unit ID field, [11-13](#)

- unit initialising
 - cold starts on STU, BSC, BSSU, DTU, BSIU, and port units, [11-42](#)
 - cold starts when corresponding mate has a failure, [11-44](#)
 - SRC warm start, [11-40](#)
 - warm starts on STU, BSC, DTU, and port units, [11-41](#)
- unit states, [11-11](#)
- Unit Status field
 - DTU Query Results window, [9-43](#)
 - MS Control Query Results window, [9-12](#)
 - MS Slice Query Results window, [9-23](#)
 - MSP transmission Query Results window, [10-29](#)
 - SNCP transmission Query Results window, [10-41](#)
 - STM1 1:8 Query Results window, [9-54](#)
- Unit {1–9, 11–19} Fail, [9-56](#)
- units
 - ARU information, [2-16](#)
 - BSSU information, [1-15](#)
 - codes, [2-31](#)
 - definitions of unit terms, [2-3](#)
 - in Main Controller subrack, [1-17](#)
 - in Matrix and Control rack, [1-16](#)
 - in Matrix and Synchronisation subrack, [1-13](#)
 - in PSA subrack, [1-28](#)
 - in PSC subrack, [1-30](#)
 - LHU information, [2-18](#)
 - masters and slaves, [11-8](#)
 - MPU information, [2-21](#)
 - MSU information, [2-23](#)
 - precautions when handling, [2-5](#)
 - PSP information, [2-19](#)
 - unlocking MC protection states, [9-71](#)
 - Update button, [4-19](#)
 - Update button and menu item on query results, [4-15](#)
 - updating records, [4-15](#)
 - updating records from a query procedure, [4-16](#)
 - User ID field, [8-38](#)
 - user interface structure, [4-8](#)
 - User Panel
 - description and illustration, [1-20](#)
 - LEDs, switches, and connectors on, [1-20](#)
 - USER PANEL connector on the ACP, [1-24](#)
 - User Panel indicator failure, [13-15](#)
 - User transaction queries, [8-37](#)
 - User Transactions Query Results window
 - field descriptions, [8-38](#)
 - graphic of, [8-38](#)
 - User Transactions window
 - field descriptions, [8-35](#)
 - graphic of, [8-35](#)
 - user-interface PC, [4-2](#)
 - users interface sessions, number of, [4-2](#)
 - Utilities menu, [4-11](#)

V

 - V.28 connections, [1-8](#)
 - V.28 connectors on User Panel, [1-21](#)
 - View Current Alarms Query Results window
 - field descriptions, [7-5](#)
 - graphic of, [7-5](#)
 - View Current Alarms window
 - field descriptions, [7-3](#)
 - graphic of, [7-3](#)
 - View Results button, [4-19](#)
 - View Results Query window
 - field descriptions, [14-4](#)
 - graphic of, [14-4](#)
 - View Test Results window
 - field descriptions, [14-2](#)
 - graphic of, [14-2](#)
 - viewing test results, [14-3](#)
 - VME ENV connector on the ARU, [2-17](#)
 - VOLcDI alarm
 - clearing, [21-220](#)
 - description, [21-219](#)
 - VOLcREP alarm
 - clearing, [21-223](#)
 - description, [21-222](#)

W

 - Wait to Restore, [10-33](#)
 - Wait To Restore Protect
 - MSP transmission Query Results window (ITU and ANSI), [10-9](#)

- MSP transmission
 - Query Results window (NTT), [10-20](#)
- Wait To Restore Protect Remote
 - MSP transmission
 - Query Results window (ITU and ANSI), [10-9](#)
 - MSP transmission
 - Query Results window (NTT), [10-20](#)
- Wait To Restore Slice {1-8}, [9-26](#)
- Wait to Restore Time field
 - SNCP transmission
 - Query Results window, [10-40](#)
- Wait To Restore Unit {1-8, 11-18}, [9-57](#)
- Wait To Restore Working
 - MSP transmission
 - Query Results window (ITU and ANSI), [10-9](#)
 - MSP transmission
 - Query Results window (NTT), [10-20](#)
- Wait To Restore Working Remote
 - MSP transmission
 - Query Results window (ITU and ANSI), [10-9](#)
 - MSP transmission
 - Query Results window (NTT), [10-20](#)
- warm starts
 - difference between cold starts and, [11-5](#)
 - SRC, [11-40](#)
 - STU, BSC, DTU, and port units, [11-41](#)
- warranties, [22-1](#)
- wildcard addresses, [5-9](#)
- windows
 - Alarm Indicator Tests, [13-6](#)
 - Automatic Laser Shutdown, [17-4](#)
 - Autonomous Messages, [8-9](#)
 - Autonomous Messages
 - Query Results, [8-16](#)
 - Background Tests View Results, [15-3](#)
 - Backup Database, [18-2](#)
 - Button Testing Test Results, [13-24](#)
 - Button Tests, [13-22](#)
 - Clear Test History, [16-2](#)
 - Defects, [8-40](#)
 - Defects Query Results, [8-43](#)
 - Diagnostic Testing Test Results, [12-88](#)
 - Diagnostic Tests, [12-18](#)
 - DTU, [9-40](#)
 - DTU Query Results, [9-43](#)
 - Fibre Assignments, [19-2](#)
 - Fibre Assignments
 - Query Results, [19-5](#)
 - LED Tests, [13-17](#)
 - Login, [4-4](#)
 - main application
 - window, information about, [4-10](#)
 - Matrix Slice, [9-20](#)
 - Matrix Slice Query Results, [9-23](#)
 - MC Control Query Results, [9-64](#)
 - MS Control, [9-9](#)
 - MS Control Query Results, [9-12](#)
- MSP transmission, [10-25](#)
- MSP transmission
 - Query Results, [10-29](#)
- paths to all, [4-8](#)
- Performance
 - Monitoring, [8-26](#)
- Performance Monitoring
 - Query Results, [8-30](#)
- shortcuts to, [4-12](#)
- SNCP transmission, [10-37](#)
- SNCP transmission
 - Query Results, [10-40](#)
- Station Alarm Control, [7-9](#)
- STM1 1:8, [9-51](#)
- STM1 1:8 Query Results, [9-54](#)
- Subrack Control, [11-15](#)
- Subrack Controller
 - Query Results, [11-17](#)
- Unit Control, [11-38](#)
- User Transactions, [8-35](#)
- User Transactions Query Results, [8-38](#)
- View Current Alarms, [7-3](#)
- View Current Alarms
 - Query Results, [7-5](#)
- View Results Query, [14-4](#)
- View Test Results, [14-2](#)
- working entity description, [9-5](#)
- Working Slice field, [9-21](#)
- worksheet file (*.xls), [8-5](#)
- wrist strap (ESD), [2-4](#)
- Wrong unit in slot state, [11-36](#)

WRONG_UNIT_AV state,
[11-12](#)

WRONG_UNIT_UN state

SRC, [11-10](#)

Unit, [11-12](#)

WS1 and WS2 connectors
on User Panel, [1-21](#), [9-67](#)

WTR field on Matrix Slice
Query Results window,
[9-23](#)

WTR field on STM1 1:8
Query Results window,
[9-54](#)

WTR Timer button, [4-19](#)

WUPcEQ alarm

clearing all units except
SRC units, [21-228](#)

clearing for SRC units,
[21-227](#)

description, [21-225](#)

flowchart, [21-226](#)

.....

X XC-CIT, [4-2](#)

XCOUPLE-COMM, [21-174](#)

XCOUPLE-TIME, [21-174](#)