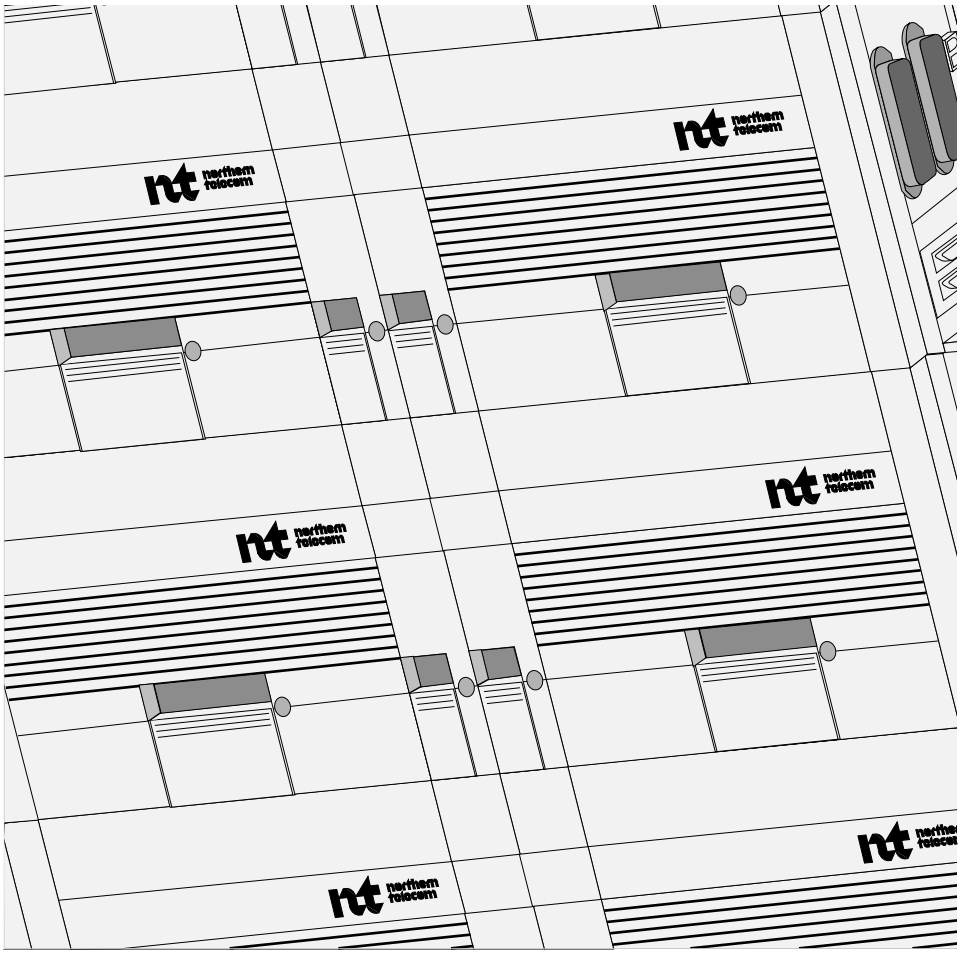
NT4K00LA **323-3001-543**

SONET Products

AccessNode

Alarm and Trouble Clearing Procedures

Issue 3.0 October 1999



NORTEL NETWORKS™

SONET Products

AccessNode

Alarm and Trouble Clearing Procedures

Document number: 323-3001-543
Document release: Issue 3.0
Date: October 1999

Copyright © 1993–1999 Nortel Networks, All Rights Reserved.

Printed in Canada

All information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.

ACCESSNODE, ACCESSNODE EXPRESS, MAP, NORTEL NETWORKS, and NORTEL are trademarks of Nortel Networks Corporation.
.

Publication history

October 1999

Standard AN17.20 release of the document. Issue 3.0.

June 1999

Standard AN17 release of the document, Issue 2.0. Changes included:

- adding clearing procedures for traffic threshold facility alarms
- adding alarms for DTAP card

February 1999

Standard AN16 release of the document. Changes included:

- adding descriptions and a procedure for clearing OPC alarms
- removing all references to FST
- adding alarms for matched nodes and duplicate network IDs and names
- adding alarms and procedures for the 8-fan cooling unit
- making minor modifications for the management by release and DS1 spurious switching features

June 1998

AN15 standard 01.01 release of the document. Includes:

- new alarms: RMM degraded link, RMM link fail, Firmware version mismatch (AIC/LAIC)
- revised alarms: VLCM degraded link, VLCM link fail

September 1997

AN14 standard 01.01 release of the document.

July 1996

AN12 standard 01.01 release of the document.

November 1995

AN11 standard 02.01 release of the document.

May 1995

An updated standard AN10 release of the document was issued. In the updated version, in Chapter 3, a correction has been made to the *Eqp LC Sync lost with NT1* alarm.

April 1995

AN10 standard release of the document.

December 1994

AN08 standard release of the document.

November 1994

AN07 reissue of standard.

April 1994

AN07 standard release of the document.

May 1993

FPW06 standard release of the document.

Contents

About this document **xxi**
Audience xxi
How to use this document xxi
References in this document xxii

Overview of alarm and trouble clearing **1-1**
Chapter contents 1-1
Procedure 1-1 Displaying alarms 1-2
Procedure 1-2 Silencing an alarm 1-5
Procedure 1-3 Manually clearing OPC alarms 1-6
Interpreting the information on an alarm screen 1-7
Alarm severity 1-7
Alarm classes and types 1-9
How to look up an alarm procedure 1-12
Example of looking up an alarm procedure 1-13
Group and slot associations 1-14
Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12 1-15
Group and slot associations for DS1, DS3, and STS-1 I/O cards 1-16
DS1 I/O numbers 1-17
DS3 I/O numbers 1-18
STS-1 I/O numbers 1-19

Alarm reporting and surveillance **2-1**
Chapter contents 2-1
Alarm hierarchies (masking relationships) 2-2
Facility alarm hierarchy 2-2
Equipment alarm hierarchy 2-5
Common equipment alarm hierarchy 2-7
Environmental alarm hierarchy 2-8
Parent equipment hierarchy 2-8

Clearing an equipment alarm **3-1**
Chapter contents 3-1
Eqp AIC 3-20
Circuit pack fail 3-20
Circuit pack mismatch 3-21
Circuit pack missing 3-22
Comm overhead clock/frame loss 3-23
Comm overhead data loss 3-24
D-link interface fail 3-26

Firmware version mismatch 3-29
Plane messaging corruption 3-30
T-link interface fail 3-31
Eqp ANX 3-33
ANX loss of comms 3-33
Circuit pack fail 3-33
Circuit pack mismatch 3-33
Shelf mismatch 3-33
Talk battery failure 3-33
Threshold 1 DS0 exceeded 3-34
Threshold 2 DS0 exceeded 3-34
Eqp ATM 3-35
Circuit pack fail 3-35
Circuit pack missing 3-35
Eqp CDS 3-36
Power filter A missing 3-36
Power filter B missing 3-39
Eqp CDSP 3-42
Access failure 3-42
Circuit pack fail 3-43
Circuit pack mismatch 3-44
Circuit pack missing 3-45
Clock failure 3-46
Eqp CE 3-47
Autoprovisioning mismatch 3-47
Both planes non-operational 3-48
CNet link fail 3-51
CNet performance degraded 3-52
Critical test alarm 3-53
Database not restored. Type Q APPROVE at NE 3-54
Entry to SONET clock freerun 3-56
Exerciser fail 3-59
Loss of data synchronization 3-60
Major test alarm 3-61
Minor test alarm 3-62
Plane A non-operational 3-63
Plane B non-operational 3-65
Ring reconfiguration in progress 3-67
Shelf assembly fail 3-68
Shelf ID bus fail 3-69
Software trap 3-70
SONET overhead data/clock loss 3-71
Timing generation primary reference fail 3-73
Timing generation secondary reference fail 3-73
Traffic upgrade in progress 3-77
Warning test alarm 3-78
User port 1 intrusion attempt 3-79
User port 2 intrusion attempt 3-79
User port 3 intrusion attempt 3-79
User port 4 intrusion attempt 3-79
Eqp DS1 3-80

Circuit pack fail 3-80
Circuit pack mismatch 3-81
Circuit pack missing 3-83
Facility provisioning mismatch 3-84
Forced switch request 3-85
Input card fail -DoNotRemove 3-86
Input card mismatch 3-87
Input card missing 3-88
Lockout request 3-89
Manual switch request 3-90
Output card fail - DoNotRemove 3-91
Output card mismatch 3-92
Output card missing 3-93
Prot bridge in card fail -DoNotRemove 3-94
Prot bridge in card mismatch 3-95
Prot bridge in card missing 3-96
Prot bridge out card fail -DoNotRemove 3-97
Prot bridge out card mismatch 3-98
Prot bridge out card missing 3-99
Protection path fail 3-101
Protection switch complete 3-105
Protection switch fail 3-106
Protection version mismatch 3-110
STS1 intercard fail 3-111
Eqp DS3 3-112
BNC I/O card 1 fail -DoNotRemove, 3-112
BNC I/O card 2 fail -DoNotRemove, 3-112
BNC I/O card 3 fail -DoNotRemove 3-112
BNC I/O card 1 mismatch, 3-113
BNC I/O card 2 mismatch, 3-113
BNC I/O card 3 mismatch 3-113
BNC I/O card 1 missing, 3-114
BNC I/O card 2 missing, 3-114
BNC I/O card 3 missing 3-114
Circuit pack fail 3-115
Circuit pack mismatch 3-116
Circuit pack missing 3-117
Forced switch 3-118
Lockout request 3-119
Manual switch request 3-120
Protection path fail 3-121
Protection switch complete 3-124
Protection switch fail 3-126
STS1 intercard fail 3-129
Switcher circuit pack mismatch 3-131
Switcher circuit pack missing 3-132
Traffic problem detected 3-133
VT connection provisioning mismatch 3-136
Eqp DTAP 3-137
Circuit pack fail 3-137
Circuit pack mismatch 3-138

Circuit pack missing 3-139
Circuit pack partial fail 3-140
Eqp ESI 3-141
End VCO range 3-141
Equipment forced switch request 3-142
Equipment lockout request 3-143
Equipment manual switch request 3-144
Equipment protection switch complete 3-145
Equipment protection switch fail 3-146
Failure to lock 3-147
Intercard failure 3-148
Subunit fail 3-149
Subunit mismatch 3-150
Subunit missing 3-151
Timing generation entry to acquire 3-152
Timing generation entry to fast 3-153
Timing generation entry to freerun 3-154
Timing generation entry to holdover 3-156
Eqp IRTU 3-158
Circuit pack fail 3-158
Circuit pack mismatch 3-159
Circuit pack missing 3-160
Common circuitry fail 3-161
Software download fail 3-163
Test head 1 fail 3-165
Test head 2 fail 3-167
Eqp ITU 3-169
Circuit pack fail 3-169
Circuit pack mismatch 3-169
Circuit pack missing 3-169
Eqp LC 3-170
Line card fail 3-170
Line card missing 3-177
Loss of power at NT1 3-178
NT1 power status changed 3-179
NT1 test mode changed 3-180
Sync lost with NT1 3-181
Eqp LIC 3-182
A-link clock driver fail 3-182
Circuit pack fail 3-184
Circuit pack mismatch 3-187
Circuit pack missing 3-188
D-link interface fail 3-190
Inter-plane fail 3-196
Plane messaging corruption 3-198
Eqp MIC 3-201
Alarm relay fail 3-201
Circuit pack fail 3-202
Circuit pack mismatch 3-203
Circuit pack missing 3-204
E2A input fail 3-205

Firmware version mismatch 3-206
LED driver fail 3-209
Local craft interface port fail 3-210
Non-volatile store fail 3-211
Non-volatile store mismatch 3-212
Orderwire fail 3-213
Parallel telemetry relay fail 3-214
Performance monitor clock fail 3-215
Protection switch relay fail 3-216
Serial telemetry port fail 3-217
Time of day clock fail 3-218
Eqp MLC 3-219
Circuit pack fail 3-219
Circuit pack mismatch 3-219
Circuit pack missing 3-219
Partial circuit pack fail 3-219
Eqp MTAC 3-220
Circuit pack fail 3-220
Circuit pack mismatch 3-221
Circuit pack missing 3-222
Eqp OC1 3-223
Rx line AIS 3-223
Rx loss of frame 3-223
Rx loss of signal 3-223
Rx RFI 3-223
Rx signal degrade 3-223
Rx signal failure 3-223
Rx section trace mismatch 3-223
STS1 Rx AIS 3-224
STS1 Rx excessive BIP error rate 3-224
STS1 Rx loss of pointer 3-224
STS1 Rx path trace mismatch 3-224
STS1 Rx RFI 3-224
STS1 Rx signal degrade 3-224
STS1 Rx signal label mismatch 3-224
STS1 Rx unequipped 3-224
VT Rx AIS 3-225
VT Rx excessive BIP error rate 3-225
VT Rx loss of pointer 3-225
VT Rx RFI 3-225
VT Rx signal degrade 3-225
VT Rx signal label mismatch 3-225
VT Rx unequipped 3-225
Eqp OC-3/OC-12 3-226
Channel match fail 3-226
Circuit pack fail 3-227
Circuit pack mismatch 3-228
Circuit pack missing 3-229
Circuit pack reach mismatch 3-230
Entry to SONET clock freerun 3-231
Fiber connection error 3-233

Firmware version mismatch 3-234
Forced switch request 3-235
Intercard failure 3-236
Laser bias current 3-239
Laser degrade 3-240
Lockout protection operation fail 3-241
Lockout request 3-242
Manual switch request 3-243
Protection oscillation control activated 3-244
Protection path fail 3-245
Protection scheme mismatch 3-247
Protection switch complete 3-248
Protection switch fail 3-249
Protection switching byte fail/Improper APS code 3-251
Receive fail 3-252
STS1 intercard fail 3-253
Switch mode mismatch 3-255
Transmission rate mismatch 3-257
Transmit fail 3-258
Unable to track clock reference 3-259
Eqp OC-12 3-260
Default K bytes 3-260
Duplicate NE ID Alarm 3-261
Duplicate NE Name 3-262
Entry to SONET clock acquire 3-264
Entry to SONET clock freerun 3-265
Entry to SONET clock holdover 3-266
Fiber loopback 3-268
Firmware corrupt 3-269
Firmware/software incompatible 3-270
Firmware trap 3-271
Intercard serial link fail 3-272
Invalid neighbor detected 3-273
Lockout protection request 3-275
Lockout working request 3-276
Maps invalid 3-277
Matchnode connection provisioning mismatch 3-278
NE id mismatch 3-279
Performance monitor clock fail 3-280
Protection switching byte/APS code inconsistent 3-281
Reference input clock fail 3-282
Ring protection suspended or unavailable 3-283
STS1 intercard fail 3-284
STS12 ring link parity error 3-285
Synchronization clock fail 3-286
System clock reference fail 3-287
VT connection provisioning mismatch 3-288
Eqp OPC 3-289
Configuration audit fail 3-289
Connection audit fail 3-291
Datasync fail 3-293

Lost peer OPC 3-294
NE DB missing/outdated 3-295
OPC alarm(s) active 3-297
OPC circuit pack fail 3-298
OPC circuit pack mismatch 3-299
OPC circuit pack missing 3-300
OPC CNET loss of signal 3-301
OPC Ethernet loss of signal 3-302
OPC hardware reset 3-305
OPC OAM software fail 3-306
OPC serial I/O card mismatch 3-307
OPC serial I/O card missing 3-308
Tape backup/Restore fail 3-309
Eqp Proc 3-312
Both C-bus access fail 3-312
C-bus-A access fail 3-313
C-bus-B access fail 3-314
Circuit pack missing 3-315
Communication processor fail 3-316
Degraded communication processor 3-317
Degraded host processor 3-318
Degraded master CBIC-A 3-319
Degraded master CBIC-B 3-320
Firmware PROM Fail 3-321
Interprocessor comm fail 3-322
Loss of data synchronization 3-323
Loss of duplex 3-324
Loss of mate communication 3-325
Eqp PSU 3-326
Circuit pack fail 3-326
Circuit pack mismatch 3-326
Circuit pack missing 3-326
Eqp SI 3-327
Circuit pack fail 3-327
Circuit pack mismatch 3-327
Circuit pack missing 3-327
Signal battery A loss 3-327
Signal battery B loss 3-327
Talk battery A loss 3-327
Talk battery B loss 3-327
Eqp SPX 3-328
Circuit pack fail 3-328
Circuit pack mismatch 3-328
Circuit pack missing 3-328
Duplex SP comms failure 3-328
Environmental alarm hw fail 3-328
ITU comms failure 3-328
ITU datasync fail 3-328
Loss of primary timing reference 3-329
Loss of secondary timing reference 3-329
SID mismatch 3-329

Software release mismatch 3-329
SP datasync fail 3-329
Timing generation entry to freerun 3-329
Upgrade in progress 3-329
Eqp STS1 3-330
BNC I/O card 1 fail 3-330
BNC I/O card 2 fail 3-330
BNC I/O card 3 fail 3-330
BNC I/O card 1 mismatch 3-331
BNC I/O card 2 mismatch 3-331
BNC I/O card 3 mismatch 3-331
BNC I/O card 1 missing 3-332
BNC I/O card 2 missing 3-332
BNC I/O card 3 missing 3-332
Circuit pack fail 3-333
Circuit pack mismatch 3-334
Circuit pack missing 3-335
Firmware failure 3-336
Firmware/software incompatible 3-337
Forced switch request 3-338
Lockout request 3-339
Manual switch request 3-340
Protection path fail 3-341
Protection switch complete 3-344
Protection switch fail 3-345
STS1 intercard fail 3-347
Switcher circuit pack mismatch 3-348
Switcher circuit pack missing 3-349
Traffic problem detected 3-350
VT connection provisioning mismatch 3-353
Eqp TAC 3-354
Circuit pack fail 3-354
Circuit pack mismatch 3-355
Circuit pack missing 3-356
Digital side fail 3-357
Metallic side fail 3-358
PGTC I/O card mismatch 3-359
Software download fail 3-360
TAP I/O card mismatch 3-362
TBP I/O card mismatch 3-363
Eqp TDM 3-364
A-link clock driver fail 3-364
Circuit pack fail 3-364
Circuit pack mismatch 3-364
Circuit pack missing 3-364
Control link fail to TDM-A 3-364
Control link fail to TDM-B 3-364
D-link interface fail 3-365
Loss of mate communication 3-365
PCM path fail to TDM-A 3-365
PCM path fail to TDM-B 3-365

TDM inter-plane fail 3-365
Eqp TIC 3-366
Backplane parity error 3-366
Circuit pack fail 3-367
Circuit pack mismatch 3-368
Circuit pack missing 3-369
Loss of signal synchronization 3-370
T-link interface fail 3-371
TR-08 circuit pack mismatch 3-373
Eqp TXC 3-374
Circuit pack failure 3-374
Circuit pack mismatch 3-375
Circuit pack missing 3-376
End VCO range 3-377
Equipment lockout request 3-378
Equipment protection switch complete 3-379
Equipment protection switch fail 3-380
Equipment prot oscillation control activated 3-382
Failure to lock 3-383
Forced equipment switch request 3-385
Forced timing reference switch request 3-386
Intercard: STS1 parity error or clock fail 3-387
Manual equipment switch request 3-389
Manual timing reference switch request 3-390
Partial circuit pack fail 3-391
Serial link failure 3-392
Sys clock src entry to freerun 3-393
Timing gen entry to acquire mode 3-395
Timing gen entry to fast mode 3-396
Timing gen entry to freerun mode 3-397
Timing gen entry to holdover mode 3-400
Timing generation primary reference fail 3-401
Timing generation secondary reference fail 3-403
Timing ref lockout request 3-405
Timing ref prot oscillation control activated 3-406
Timing ref prot switch complete 3-407
Timing ref prot switch fail 3-408
Eqp UE 3-409
TDM firmware mismatch 3-409
Upgrade in progress 3-409

Clearing a facility alarm **4-1**

Chapter contents 4-1
Fac COMM 4-10
Faulty path 4-10
No active path 4-12
OMC link fail 4-13
OMC performance degraded 4-16
SONET DCC link fail 4-19
SONET DCC performance degraded 4-21
Fac DS1 4-22

CSU line loopback 4-22
Facility loopback 4-22
Network loopback 4-22
Terminal loopback 4-22
High traffic threshold exceeded 4-23
Line Rx CV threshold 1, 2, 4-24
Line Rx ES threshold 1, 2, 4-24
Line Rx SES threshold 1, 2 4-24
Loopback 4-27
Low traffic threshold exceeded 4-28
Path Rx CV threshold 1, 2 4-29
Path Rx ES threshold 1, 2 4-29
Path Rx SAS threshold 1, 2 4-29
Path Rx SES threshold 1, 2 4-29
Path Rx UAS threshold 1, 2 4-29
PRI link OOS 4-32
Rx AIS 4-33
Rx babbling 4-34
Rx bipolar violation > 10E-3 4-35
Rx bipolar violation > 10E-4 4-38
Rx loss of frame 4-39
Rx loss of signal 4-42
Rx yellow 4-44
STS1 path CV threshold 1, 2 4-45
STS1 path ES threshold 1, 2 4-45
STS1 path SES threshold 1, 2 4-45
STS1 path UAS threshold 1, 2 4-45
STS1 Rx path trace failure 4-50
STS1 Rx RFI 4-53
STS1 Rx unequipped 4-55
STS1 signal label mismatch 4-57
VT Rx AIS 4-58
VT Rx loss of pointer 4-60
VT Rx RFI 4-64
VT Rx unequipped 4-66
Fac DS3 4-68
Frequency out of range 4-68
Line FE CV threshold 1, 2 4-70
Line FE ES threshold 1, 2 4-70
Line FE SES threshold 1, 2 4-70
Line FE UAS threshold 1, 2 4-70
Line Rx CV threshold 1, 2 4-71
Line Rx ES threshold 1, 2 4-71
Line Rx SES threshold 1, 2 4-71
Loopback 4-73
Parity error rate >10E-6 4-74
Path Rx AISS threshold 1, 2 4-75
Path Rx CV threshold 1, 2 4-75
Path Rx ES threshold 1, 2 4-75
Path Rx SES threshold 1, 2 4-75
Path Rx SEFS threshold 1, 2 4-75

Path Rx UAS threshold 1, 2 4-75
Path Tx AISS threshold 1, 2 4-79
Path Tx CV threshold 1, 2 4-79
Path Tx ES threshold 1, 2 4-79
Path Tx SES threshold 1, 2 4-79
Path Tx SEFS threshold 1, 2 4-79
Path Tx UAS threshold 1, 2 4-79
Rx AIS 4-82
Rx bipolar violation > 10E-3 4-83
Rx loss of frame 4-85
Rx loss of signal 4-87
STS1 path FE CV threshold 1, 2 4-89
STS1 path FE ES threshold 1, 2 4-89
STS1 path FE SES threshold 1, 2 4-89
STS1 path FE UAS threshold 1, 2 4-89
STS1 Rx path trace failure 4-90
STS1 Rx RFI 4-93
STS1 Rx unequipped 4-94
STS1 signal label mismatch 4-96
Tx AIS 4-97
Tx loss of frame 4-98
Fac DSX1 4-100
Facility loopback 4-100
Rx AIS 4-100
Rx babbling 4-100
Rx bipolar violation > 10E-3 4-100
Rx bipolar violation > 10E-4 4-100
Rx loss of frame 4-100
Rx loss of signal 4-100
Rx yellow 4-100
Terminal loopback 4-100
Fac ESI 4-101
Bipolar violation 4-101
Degraded clock carrier 4-102
Degraded timing reference 4-103
Loss of frame 4-104
Loss of signal 4-106
Oscillating sync status message 4-108
Reference forced switch request 4-109
Reference manual switch request 4-110
Reference switch complete 4-111
Reference switch fail 4-112
Rx AIS 4-113
Timing reference interface fail 4-114
Tx AIS 4-115
Undefined sync status message 4-118
Fac HDSL 4-119
ES threshold exceeded 4-119
Loopback 4-119
Loss of Sync 4-119
Margin threshold exceeded 4-119

Fac OC-12 4-120
Inter-ring both feeds fail 4-120
Inter-ring forced switch request 4-121
Inter-ring protection switch complete 4-122
RX inter-ring secondary feed fail 4-123
TX loss of inter-ring secondary feed 4-124
Fac OC-3/OC-12 4-125
Laser bias current 4-125
Line RFI 4-126
Line Rx CV threshold 1, 2 4-127
Line Rx ES threshold 1, 2 4-127
Line Rx SES threshold 1, 2 4-127
Line Rx UAS threshold 1, 2 4-127
Sect Rx CV threshold 1, 2 4-127
Sect Rx ES threshold 1, 2 4-127
Sect Rx SES threshold 1, 2 4-127
Sect Rx SEFS threshold 1, 2 4-127
Loss of frame 4-135
Rx AIS 4-139
Rx loss of signal 4-140
Section Rx optical power threshold 4-144
Signal degrade 4-145
Signal fail 4-148
STS1 Rx AIS 4-152
STS1 Rx loss of pointer 4-156
STS1 Rx unequipped 4-162
Fac STS1 4-163
Line Rx BCV threshold 1, 2 4-163
Line Rx BES threshold 1, 2 4-163
Line Rx BSES threshold 1, 2 4-163
Line Rx CV threshold 1, 2 4-163
Line Rx ES threshold 1, 2 4-163
Line Rx SES threshold 1, 2 4-163
Line Rx UAS threshold 1, 2 4-163
Loopback 4-167
Rx bipolar violation >10E-3 4-168
Rx loss of frame 4-171
Rx loss of pointer 4-174
Rx loss of signal 4-175
Rx Line AIS 4-178
Rx RFI 4-179
STS1 Rx AIS 4-180
PRI link OOS 4-183
Rx loss of frame 4-184
Fac TIC 4-187
STS1 Rx RFI 4-187
STS1 Rx unequipped 4-188
TR-08 System [1 … 21] far end major 4-194
TR-08 System [1 … 21] loss of Rx DDL 4-195
TR-08 System [1 … 21] Rx fail 4-202
VT Path signal label mismatch 4-203

VT Rx AIS 4-204
VT Rx loss of pointer 4-207
VT Rx RFI 4-212
VT Rx unequipped 4-215

Clearing an environmental alarm 5-1
Chapter contents 5-1
Env ANX 5-3
Remote environmental critical 5-3
Remote environmental major 5-3
Remote environmental minor 5-3
Env CE 5-4
Fan 1 fail, 5-4
Fan 2 fail, 5-4
Fan 3 fail 5-4
Fan 1 fail, 800A 5-5
High bay temperature 5-7
High CE shelf temperature 5-10
Talk battery filter fail 5-13
Telemetry input 1-11 5-14
48V battery A CE supply fail 5-15
48V battery B CE supply fail 5-18
48V CDS breaker tripped ext bay 5-21
48V CDS breaker tripped main bay 5-22
48V CE, CU or TB CE breaker tripped main bay 5-23

Troubleshooting PGTC/MTA 6-1
Chapter contents 6-1
Troubleshooting PGTC/MTA access failures 6-2

Interpreting an LED or lamp 7-1
Chapter contents 7-2
Status of all active and fail LEDs 7-4
Line drawer (NT4K21) 7-7
Fail (red) 7-7
Processor circuit pack (NT4K52) 7-8
Fail (red) 7-8
Maintenance interface circuit pack (NT4K53) 7-9
CU (yellow) 7-9
Fail (red) 7-9
Init (yellow) 7-9
LckOut (yellow) 7-9
LoopBk (yellow) 7-10
Temp (red) 7-10
TestFail (red) 7-10
TestRun (yellow) 7-10
Test access card (NT4K54) 7-11
Fail (red) 7-11
Access interface card (NT4K55) 7-12
Fail (red) 7-12
Transport interface card (NT4K56) 7-13
Fail (red) 7-13

Integrated remote test unit (NT4K57) 7-14
Fail (red) 7-14
Copper distribution shelf power (NT4K62AA) 7-15
Fail (red) 7-15
Epsilon 2-wire station line card (NT4K65AA) 7-16
Fail (red) 7-16
Omega 2-wire station line card (NT4K67AB) 7-17
Fail (red) 7-17
Omega 2-wire office line card (NT4K68AA) 7-18
Fail (red) 7-18
Omega 4-wire line card (NT4K69AA) 7-19
Fail (red) 7-19
Narrowband line interface card (NT4K70AA) 7-20
Fail (red) 7-20
Metallic test access card (NT4K73AA) 7-21
Fail (red) 7-21
Metallic test access card (NT4K73CA) 7-22
Fail (red continuous or red blinking) 7-22
Omega 6- 8-wire line card (NT4K77AA) 7-23
Fail (red) 7-23
OC-3 (Optical carrier level 3) (NT7E01) 7-24
Fail (red) 7-24
LOS (yellow) 7-24
OC-12 (Optical carrier level 12) (NT7E02) 7-25
Fail (red) 7-25
LOS (yellow) 7-25
OC12 optical interface circuit pack (NT7E05) 7-26
Fail (red) 7-26
LOS (yellow) 7-26
DS1/VT mapper (NT7E04) 7-27
Fail (red) 7-27
DS3/STS mapper (NT7E08) 7-28
Fail (red) 7-28
STS-1 interface card (NT7E09) 7-29
Fail (red) 7-29
OPC (Operations Controller) (NT7E24) 7-30
Unit fail (red) 7-30
ELAN Fail (yellow) 7-30
CNET Fail (yellow) 7-30
External synchronization interface (NT7E27) 7-31
Fail (red) 7-31
OPC (Operations Controller) tape drive unit 7-32
Interpreting breaker interface panel (BIP) LEDs 7-34
ABM BIP indicators 7-34
TBM BIP indicators 7-34

Performing diagnostic tests **8-1**

Chapter contents 8-1
Procedure 8-1 Manually testing the protection groups on a shelf 8-2
Procedure 8-2 Manually exercising the processor 8-4
Procedure 8-3 Performing a lamp test from the NEUI 8-6

Procedure 8-4 Performing a lamp test using the ACO/LAMP TEST button 8-8
Procedure 8-5 Performing a manual diagnostic test 8-10
Procedure 8-6 Setting or releasing a loopback on a DS1 or DS3 facility 8-14
Procedure 8-7 Manually switching processor activity from active to standby 8-17
Procedure 8-8 Manually restarting the processor 8-19
Procedure 8-9 Manually restarting the shelf 8-23
Procedure 8-10 Resetting a line card 8-26
Procedure 8-11 Diagnosing failed CDS circuit packs 8-28
Procedure 8-12 Generating alarms for testing purposes 8-32

Index **9-1**

About this document

This document has procedures for clearing network element trouble conditions reported by alarms, alerts, and trouble log reports.

> ***Note:*** If the alarm relay card is removed, the three alarm lamps and the power lamp on the breaker interface panel will not illuminate, and the cuttable and noncuttable office alarms will not be generated.

The OPC procedures in this document (although CMT-based) can be performed from a graphical terminal, however you must substitute the CMT keystrokes that are provided in the procedures with the graphical equivalent. Refer to the Graphical Reference card that is provided in the sleeve of this volume, or in *OPC User Interface Description*, 323-3001-301, in *Operations, Administration, and Provisioning,* Volume 4A.

Commands, parameter, and response conventions used in procedures are described in *OPC User Interface Description*, 323-3001-301, in *Operations, Administration, and Provisioning,* Volume 4A.

Audience

This document is for maintenance technicians and Northern Telecom technicians to use as a guide when monitoring system performance.

How to use this document

The procedures in this document can be used at any time and in any order. The specific alarms are documented in alphabetical order and can easily be found.

References in this document

This document refers to the following documents:

***Engineering, Configuration, and Ordering*, Volume 1**

- *Engineering and Ordering Information*, 323-3001-032
- *Mapper Layouts Planning Guide*, 323-3001-154

Commissioning and Testing, Volume 3

Operations, Administration, and Provisioning, Volume 4A

- *Network Element User Interface Description*, 323-3001-300
- *OPC User Interface Description*, 323-3001-301
- *System Administration Procedures*, 323-3001-302
- *Data Administration Procedures*, 323-3001-304

Operations, Administration, and Provisioning, Volume 4B

- *Provisioning and Operations Procedures*, 323-3001-310
- *Line Card Provisioning Procedures*, 323-3001-315
- *Line Card Testing Procedures*, 323-3001-316

Maintenance, Volume 5B

- *Log Report Manual*, 323-3001-840

Maintenance, Volume 5C

- *Network Surveillance Procedures*, 323-3001-510
- *Performance Monitoring Procedure*s, 323-3001-520
- *Routine Maintenance Procedures*, 323-3001-546
- *Module Replacement Procedures*, 323-3001-547

Separately Bound

- *Bay in Central Office Installation Manual for ABM*, 323-3001-201
- *Series 800A Outside Plant Cabinet Description Manual*, 323-3001-118
- *Series 800A Outside Plant Cabinet Installation Manual*, 323-3001-210
- *Installing or Replacing the Digital Test Access Pair*

AccessNode Express documents

- *AccessNode Express Commissioning and OAM&P, 323-3051-220*
- *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543
- *AccessNode Express Commissioning Quick Reference Guide*

Overview of alarm and trouble clearing

This chapter describes how to begin clearing an alarm, alert, trouble log report, or a circuit pack alarm LED. It includes a procedure for displaying active alarms and a procedure for silencing alarms. The chapter also describes how to interpret alarm information and how to determine group and slot associations for various shelves, cards, and mappers.

Chapter contents

This chapter includes the following procedures:

Procedure	Task	See
Procedure 1-1	Displaying alarms	page 1-2
Procedure 1-2	Silencing an alarm	page 1-5
Procedure 1-3	Manually clearing OPC alarms	page 1-6

In addition, this chapter includes the following topics:

Topic	See
Interpreting the information on an alarm screen	page 1-7
How to look up an alarm procedure	page 1-12
Group and slot associations	page 1-14

Note: To perform maintenance on power feeds, see *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

Procedure 1-1
Displaying alarms

Use this procedure to view network element alarms from the operations controller (OPC) user interface or the network element (NE) user interface.

Note: The autologout feature logs you out of the network element in five seconds if one of the following communication problems occurs:

- The terminal is powered off.
- A problem such as a disconnected RS-232 cable to the local craft access panel (LCAP) causes the data terminal equipment (DTE) connection to be lost.
- A problem such as a disconnected MODEM cable to the side interconnect left causes the data communication equipment (DCE) connection to be lost.

Requirements

You must log on to the OPC user interface or the network element user interface.

Read the command conventions in *Data Administration Procedures,* 323-3001-304, in *Operations, Administration, and Provisioning,* Volume 4A.

Action

Step	Action

If you are logged in to	Then go to
the OPC user interface	step 1
the NE user interface	step 7

—continued—

Procedure 1-1 (continued)
Displaying alarms

Step	Action
1	Display the Session Manager and open the NE Login Manager tool. *The NE Login Manager tool main window appears.*
2	To display the chooser menu, press **Ctrl_L** ***/*** (or Keypad **3**). *The chooser menu appears with the first item highlighted.*
3	Press the arrow keys to move to the network element you want to log in to, then press **Space** (or Keypad **0**). *The ID and name of the selected network element appear in the Network Element field.*

4	Tab to the **Login** button, then press **Ctrl_A** (or Keypad **0**).
	A screen appears with the following prompt:
	`Enter username:`
	`>`
	If this prompt does not appear, a connection is not possible at this time. Try later or use the Event Browser tool to look for a possible cause (such as software downloading).

5	Log in to the network element by entering:
	<username>↵
	where
	<username> your network element user name
	A screen appears with the following prompt:
	`Enter password:`
	`>`

6	Enter: **<password>**↵ where <password> your network element password *If the username and password are correct, the Network Element Status screen appears.* Go to step 8.

—continued—

Procedure 1-1 (continued)
Displaying alarms

Step	Action
7	To display the Network Element Status screen, enter: **mapci;fwpui**↵ *The Network Element Status screen appears.*
8	To display a list of active alarms for the network element, enter: **alarms**↵ *The system displays a list of alarms in decreasing order of severity. The alarm report ID number appears under the Alm heading.*
9	Note the following information about an alarm: • class of alarm (Eqp, Fac, or Env) under the Class heading on the Active Alarms screen • type of alarm (such as DS1, COMM, OC12) under the Type heading • alarm text (such as Loss of frame) under the Reason heading • unit (such as G1 or G2) under the Unit heading ***Note 1:*** See "Interpreting the information on an alarm screen" on page 1-7 for information about using the alarm class, type, and reason to clear alarms. ***Note 2:*** See "Group and slot associations" for information about the alarm unit. ***Note 3:*** If you want to display detailed information about an alarm, from the Active Alarms screen enter: **dtlalms <alarm>**↵ where <alarm> alarm report ID number: **0** to **399** *The Detailed Alarm Report screen appears.*
10	Return to the Active Alarms screen by entering: **quit**↵

—end—

Procedure 1-2
Silencing an alarm

Use this procedure to silence an audible alarm in one of the following ways:

- by pressing the ACO/LT button on the local craft access panel (LCAP)
- by using the ACO (alarm cut off) command available at any network element user interface screen
- by using the remote ACO on the breaker interface panel (BIP) wirewrap pins.

Action

Step	Action
1	To use the ACO user interface command, complete the following substeps: **a.** Log in to the network element that has the active audible alarm. **b.** From any screen, enter: **sil.**↵
2	To use the ACO/LT button on the LCAP, press it to silence audible alarms.
3	To use the ACO at the remote fiber terminal (RFT), momentarily short the BIP "ACO" wirewrap pins together. ***Note:*** An equipment failure of the maintenance interface card (MIC) can cause the alarm cut off (ACO) to fail. If the alarm cut off fails, you can silence the alarm by removing the alarm relay card.

—end—

Procedure 1-3
Manually clearing OPC alarms

Use this procedure to manually clear alarms generated by the OPC after you correct the cause of the alarm but before the alarm automatically clears. Alarms clear automatically 1 to 2 minutes after the cause of the alarm has been corrected.

You can display OPC alarms using the OPC Alarm Monitor or Event Browser tools.

Requirements

Before starting this procedure, you must log in to the OPC with access privileges for the OPC Alarm Provisioning tool. For log-in instructions and an overview of the OPC user interface, see *OPC User Interface Description*, 323-3001-301, in *Operations, Administration, and Provisioning*, Volume 4A.

Action

Step	Action
1	From the User Session Manager, open the OPC Alarm Provisioning tool by moving the cursor to the tool name and pressing **Ctrl_A** (or Keypad **0**). *The OPC Alarm Provisioning main window appears.*
2	Tab to the list of all OPC alarms.
3	Using the arrow keys, move to the alarm you want to clear.
4	Display the list item menu by pressing **Ctrl_L** (or Keypad **Enter**). *The list item menu appears.*
5	Move to the **Manual clear** command by using the arrow keys, then press **Space** (or Keypad **0**). *A confirmation dialog appears.*
6	Tab to the **Yes** button, then press **Ctrl_A** (or Keypad **0**).
7	If you are displaying the alarm in the OPC Alarm Monitor or Event Browser main window, refresh the screen display to show that the alarm status has now changed.
8	Close the tool by pressing **Esc**.

—end—

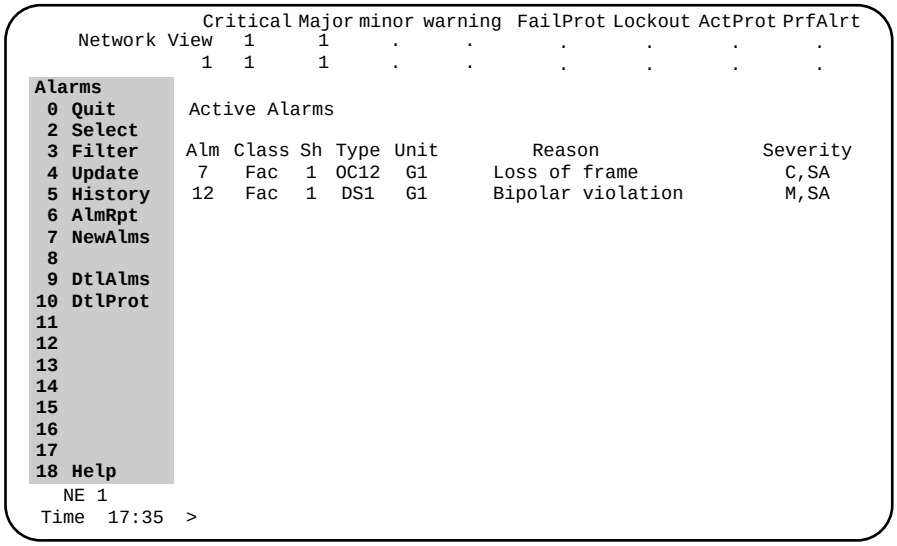
Interpreting the information on an alarm screen

This section explains how to interpret the information on the Active Alarms screen.

Figure 1-1 shows a typical Active Alarms screen.

Figure 1-1
Typical alarm screen

SC-10319



Alarm severity

AccessNode categorizes alarms by severity: critical, major, minor, and warning. It further defines alarms as service-affecting or not service-affecting. You can use the severity codes to prioritize troubleshooting. Table 1-1 on page 1-8 lists and describes the alarm severities listed under severity on the screen.

> ***Note:*** Always clear service-affecting alarms first, starting with the most critical alarms.

Table 1-1
Alarm severity

Severity screen symbols	What they mean	What to do about them
C (Critical)	The most severe alarms. A critical alarm has the potential to affect 128 (DS0) customers, for example, loss of both OC-12 facilities.	Repair immediately
M (Major)	Not as severe as critical alarms, but still requires immediate attention. A major alarm has the potential to affect 24 or more (DS0) customers, for example, loss of a DS1 facility.	Investigate immediately
m (minor)	Not as severe as major alarms, but still indicates a problem that may escalate. A minor alarm has the potential to affect 23 or fewer (DS0) customers, for example, failure of a common-equipment circuit pack.	Investigate at next opportunity
w (warning)	The least severe alarm. A warning indicates a degradation of service or the completion of an event, for example, a problem at an upstream site.	Investigate during next maintenance activity
SA (service-affecting)	Service to one or more clients is interrupted.	Investigate and repair immediately
nsa (not service-affecting)	Clients are unaware of the fault.	Investigate and repair at next opportunity
Clear	The alarm has been cleared.	

Alerts

An alert indicates that a performance monitoring threshold has been crossed. An alert is less severe than an alarm and does not affect service, but it indicates a condition that requires further investigation. The severity for all alerts is indeterminate, not service-affecting (i, nsa). However, if you have provisioned an alert to raise an alarm, the severity is warning, not service-affecting (w, nsa).

Depending on your provisioning, performance alerts can be either alerts or alarms. This document treats all performance alerts as facility (Fac) alarms.

Note 1: See “Clearing a facility alarm” on page 4-1 for directions to clear alerts.

Note 2: See *Performance Monitoring Procedures*, 323-3001-520, in *Maintenance*, Volume 5C, for procedures and detailed descriptions of performance monitoring.

Note 3: See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B, for directions to provision performance monitoring thresholds.

Alarm classes and types

In addition to classifying alarms by severity, AccessNode categorizes alarms by class and type. Table 1-2 lists and describes the alarm classes. All alarms fall within one of these classes, which appear under the Class heading on the Active Alarms screen.

Table 1-2
Alarm classes

Class screen symbols	What they mean
Fac	Facility alarm
Eqp	Equipment alarm
Env	Environment alarm

Alarms within a class are further organized by alarm type, which appears under the Type heading on the Active Alarms screen. Table 1-3 lists and describes the alarm types for each of the three alarm classes.

Table 1-3
Alarm types

Alarm class	Alarm type	Description
Eqp	AIC	Access interface card
	ANX	AccessNode Express shelf
	CDS	Copper-distribution shelf
	CDSP	Copper-distribution shelf power
	CE	Common-equipment (refers to shelf)
	DS1	DS1 transport (1.544 Mb/s)
	DS3	DS3 transport (44.736 Mb/s)
	DTAP	Digital test access pair
	STS1	STS-1 transport (51.84 Mb/s)
	ESI	External synchronization interface
	IRTU	Integrated remote test unit
	ITU	Integrated test unit
	LC	Line card

—continued—

Table 1-3 (continued)
Alarm types

Alarm class	Alarm type	Description
Eqp (cont.)	LIC	Line interface card
	MIC	Maintenance interface card
	MTAC	Metallic test access card
	OC3	OC-3 transport (155.520 Mb/s)
	OC12	OC-12 transport (622.080 Mb/s)
	OPC	Operations controller
	Proc	Processor circuit pack
	PSU	Power supply unit
	SPX	Shelf processor
	STS1	STS circuit pack
	TAC	Test access card
	TIC	Transport interface card
	TXC	Timing and cross-connect card
Fac	COMM	Communication channel or link
	DS1	DS1 traffic
	STS1	STS-1 traffic
	DS3	DS3 traffic
	ESI	External synchronization interface
	OC-3	OC-3 transport
	OC-12	OC-12 transport
	Path	Communication path
	STSn	STS path
	STS1	STS1 path
	TIC	STS1, TR08, and VT facilities
Env	ANX	AccessNode Express Shelf
	CE	Common equipment
—end—		

How to look up an alarm procedure

The following chapters of this book contain procedures for clearing alarms:

Chapter 3	Equipment alarms
Chapter 4	Facility alarms
Chapter 5	Environment alarms

Each chapter organizes the alarms by alarm type (Eqp AIC, Eqp CDS, Eqp CDSP, for example). Within alarm type, alarms are organized alphabetically by the alarm text. Table 1-4 lists the organization of the CDSP equipment alarms in Chapter 3.

Table 1-4
Eqp CDSP alarms

Alarm	See
Access failure	page 3-42
Circuit pack fail	page 3-43
Circuit pack mismatch	page 3-44
Circuit pack missing	page 3-45
Clock failure	page 3-46

Example of looking up an alarm procedure

The first alarm listed in Figure 1-1 on page page 1-7 is:

```
Class  Sh  Type  Unit    Reason
 Fac   1   OC12   G1     Loss of frame
```

To find the correct procedure to clear this alarm, you would complete the following steps:

1 Go to Chapter 4 of this book because it contains procedures for facility (Fac) alarms.

2 Look up `Loss of frame` in the OC-3/OC-12 alarms table at the beginning of Chapter 4.

Note: Check the alarm type when you look up a procedure. Some alarms (for example, Circuit pack missing) occur for more than one alarm type. Make sure the alarm class, type, and text all match before you select a procedure.

3 Go to the page that documents the alarm clearing procedure for OC12 Loss of frame.

Note: If you cannot find the alarm in this book, see *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543 for ANX voice module alarms.

Group and slot associations

Many alarm clearing procedures in this book require you to enter a group number (G1 or G2) as part of a command. The group number depends on the shelf type and function, the mapper type, and its slot location. Tables 1-5 through 1-10 on pages 1-15 through 1-19 describe the associations between groups and slots.

Note: The following tables do not imply that all slots are available for your configuration. For details about the capacity for each configuration, see the *Mapper Layouts Planning Guide*, 323-3001-154, in the *Engineering, Configuration, and Ordering Guide*, Volume 1.

Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12

Table 1-5 summarizes the group and slot associations for different mappers and shelves.

Table 1-5
Group and slot association matrix

Mapper and shelf function		Mapper slot																		
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
DS1	DS1-fed ABM	G1	G2	P	G4	G5	G6													
	ABM FCOT or FCOT_BLSR	G1	G2	P	G4	G5	G6	G7	G8											
	TBM FCOT			G3	G4							G5	G6	P	G8	G9	G10	G11	G12	
	TBM FCOT_BLSR	G1	G2	G3	G4							G5	G6	P	G8	G9	G10	G11	G12	
	TBM TN_BLSR	G1	G2	G3	G4							G5	G6	G7	G8	G9	G10	G11	G12	P
DS3	ABM	P	S	G1		G2		G3												
	TBM FCOT	P	S									G1		-		G3		G4		
	TBM FCOT_BLSR or TN_BLSR	P	S									G1		G2*		G3		G4		
STS-1	TN_BLSR		S	P								G1		G2		G3		G4		
OC-3	ABM tributary	G3		G4		G1S		G2S												
	TBM tributary	G3		G4		G1S		G2S				G5		G6		G7		G8		
	Feeder									G1	G2									
OC-12	Feeder									G1	G2									
OC-12 VTBM	Feeder									G1	G2									
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**

* For DS3 TBM FCOT_BLSR fiber-fed shelves, this group is available only if no DS1s are provisioned for that shelf.

Group and slot associations for DS1, DS3, and STS-1 I/O cards

For some tasks, you must know the slot numbers of the input and output cards. Use the following tables to determine the I/O slots for the mapper you need.

If you are provisioning	For this shelf type	Then see
DS1 equipment	Access bandwidth manager shelf (ABM)	Table 1-6
	Transport bandwidth manager shelf (TBM)	Table 1-7
DS3 equipment	ABM	Table 1-8
	TBM	Table 1-9
STS-1 equipment	TBM	Table 1-10

For DS1, DS3, and STS-1 circuit packs, Tables 1-6 through 1-10 show the association between mappers in the lower level of the common equipment shelf and input/output cards in the upper level.

For example, DS1 circuit pack group G1 refers to the group of modules including the working DS1/VT mapper circuit pack in slot 1 and its corresponding DS1 input/output cards in slots 30 and 32. Similarly, DS1 circuit pack group P refers to the group of modules including the protection DS1/VT mapper circuit pack in slot 3 and the DS1 protection bridge cards in slots 34 and 36.

DS1 I/O numbers

Table 1-6 lists the DS1 circuit pack groups for the ABM shelf functions. It also shows the association between mappers in the lower level of the shelf and input/output cards in the upper level.

Table 1-6
ABM DS1 mapper, group, and I/O numbers

Shelf function	Group or I/O slot	Mapper slot																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	-
RFT RFT_BLSR FCOT FCOT_BLSR	Group	g1*	g2*	P*	g4*	g5*	g6*	g7	g8											
	Input slot	30*	31*	34p*	35*	38	39	42	43											
	Output slot	32*	33*	36p*	37*	40	41	44	45											

Note 1: * DS1 equipment allowed in a DS1-fed ABM shelf.

Note 2: The symbol “p” in the DS1 input and output slots denotes a protection bridge card.

Note 3: The feeder occupies slots 9 and 10. If an operations controller (OPC) is installed, it occupies slots 5 through 8.

Table 1-7 lists the DS1 circuit pack groups for the different TBM shelf functions. It also shows the association between mappers in the lower level of the shelf and input/output cards in the upper level.

Table 1-7
TBM DS1 mapper, group, and I/O numbers

Shelf function	Group or I/O slot	Mapper slot																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
FCOT	Group			g3	g4							g5	g6	P	g8	g9	g10	g11	g12	
	Input slot			34	35							38	39	42p	43	46	47	50	51	
	Output slot			36	37							40	41	44p	45	48	49	52	53	
FCOT_BLSR	Group	g1*	g2*	g3	g4							g5	g6	P	g8	g9	g10	g11	g12	
	Input slot	30*	31*	34	35							38	39	42p	43	46	47	50	51	
	Output slot	32*	33*	36	37							40	41	44p	45	48	49	52	53	
TN_BLSR	Group	g1*	g2*	g3	g4							g5	g6	g7	g8	g9	g10	g11	g12	P
	Input slot	30*	31*	34	35							38	39	42	43	46	47	50	51	-
	Output slot	32*	33*	36	37							40	41	44	45	48	49	52	53	-

Note 1: * FCOT_BLSR and TN_BLSR shelves can contain two additional DS1 working groups (compared to an FCOT) when DS3 protection mappers are not used in slots 1 and 2. The two additional DS1 working groups are g1 (slots 1, 30, 32) and g2 (slots 2, 31, 33).

Note 2: The symbol “p” in the DS1 input and output slots denotes a protection bridge card.

Note 3: The feeder occupies slots 9 and 10. If an OPC is installed, it occupies slots 5 through 8.

DS3 I/O numbers

Table 1-8 lists the DS3 circuit pack groups for the ABM shelf functions. It also shows the association between mappers in the lower level of the shelf and input/output cards in the upper level.

Table 1-8
ABM DS3 mapper, group, and I/O numbers

Shelf function	Group or I/O slot	Mapper slot																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	-
RFT	Group	P	S	g1	—	g2	—	g3	—											
RFT_BLSR	I/O slots	—	—	34		38		42												
FCOT		—	—	35		39		43												
FCOT_BLSR		—	—	36		40		44												

Note 1: The feeder occupies slots 9 and 10. If an OPC is installed, it occupies slots 5 through 8.

Note 2: The symbol “P” in slot 1 denotes a protection mapper; the symbol “S” in slot 2 denotes a protection switch card.

Table 1-9 lists the DS3 circuit pack groups for the TBM shelf functions. It also shows the association between mappers in the lower level of the shelf and input/output cards in the upper level.

Table 1-9
TBM DS3 mapper, group, and I/O numbers

Shelf function	Group or I/O slot	Mapper slot																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
FCOT	Group	P	S	—	—							g1	—	g2*	—	g3	—	g4	—	—
FCOT_BLSR	I/O slots	—	—									38		42*		46		50		
TN_BLSR		—	—									39		43*		47		51		
		—	—									40		44*		48		52		

Note 1: * This group is available for FCOT_BLSR shelves that have no DS1s provisioned.

Note 2: The feeder occupies slots 9 and 10. If an OPC is installed, it occupies slots 5 through 8.

Note 3: The symbol “P” in slot 1 denotes a protection mapper; the symbol “S” in slot 2 denotes a protection switch card.

STS-1 I/O numbers

Table 1-10 lists the STS-1 circuit pack groups for the TBM shelf functions. It also shows the association between mappers in the lower level of the shelf and input/output cards in the upper level.

Table 1-10
TBM STS-1 interface, group, and I/O numbers

Shelf function	Group or I/O slot	Mapper slot																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
TN_BLSR	Group	—	S	P	—							g1	—	g2	—	g3	—	g4	—	—
	I/O slots	— — —	— — —									38 39 40		42 43 44		46 47 48		50 51 52		

Note 1: The feeder occupies slots 9 and 10. If an OPC is installed, it occupies slots 5 through 8.

Note 2 The symbol “P” in slot 3 denotes a protection mapper; the symbol “S” in slot 2 denotes a protection switch card.

Alarm reporting and surveillance

Whenever possible, AccessNode correlates alarm indications to present only one alarm point per event. It screens alarms through a hierarchy and eliminates the related alarm indications. As a result, lower-level alarm points are masked if a higher-level alarm point is raised. This chapter describes the alarm hierarchies and their relationships to each other.

AccessNode provides single-ended maintenance is provided, which means you can issue commands from one network element to be executed at another network element within the system.

Note 1: Shelf alarm monitoring is not available while you reset processor circuit packs or download software.

Note 2: See *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C for the following information:

- directions to display alarms for the network elements within an operations controller's (OPC) span of control
- a summary of the OPC network surveillance tools

Chapter contents

This chapter contains the following topics:

Topic	See
Alarm hierarchies (masking relationships)	page 2-2
Facility alarm hierarchy	page 2-2
Equipment alarm hierarchy	page 2-5
Common equipment alarm hierarchy	page 2-7
Environmental alarm hierarchy	page 2-8
Parent equipment hierarchy	page 2-8

Alarm hierarchies (masking relationships)

AccessNode has four alarm hierarchies: facility alarm, equipment alarm, common-equipment alarm, and environment alarm. The following topics describe the hierarchies and how they report alarms.

Facility alarm hierarchy

Figures 2-1 through 2-3 show the complete hierarchy for facility alarms.The arrows represent a general relationship. Not every alarm lower in the hierarchy is masked, but in general, circuit pack failures mask intercard failures.

Note: OC-12 equipment alarms mask all OC-12 and STS-1 facility alarms.

Example of a DS1 or DS3 facility alarm

When a DS1 facility receives an alarm indication signal (Rx AIS), a loss of frame (LOF) is also detected. However, the AIS alarm is raised and the LOF alarm is suppressed because the AIS alarm has a higher priority. In addition, the AIS in a DS1 facility is an unframed signal, so the LOF is meaningless. When a DS3 facility detects a LOF, the AIS is not detected because the AIS indication is part of the framed signal.

Figure 2-1 (part 1 of 3)
Facility alarm hierarchies

PC-11499

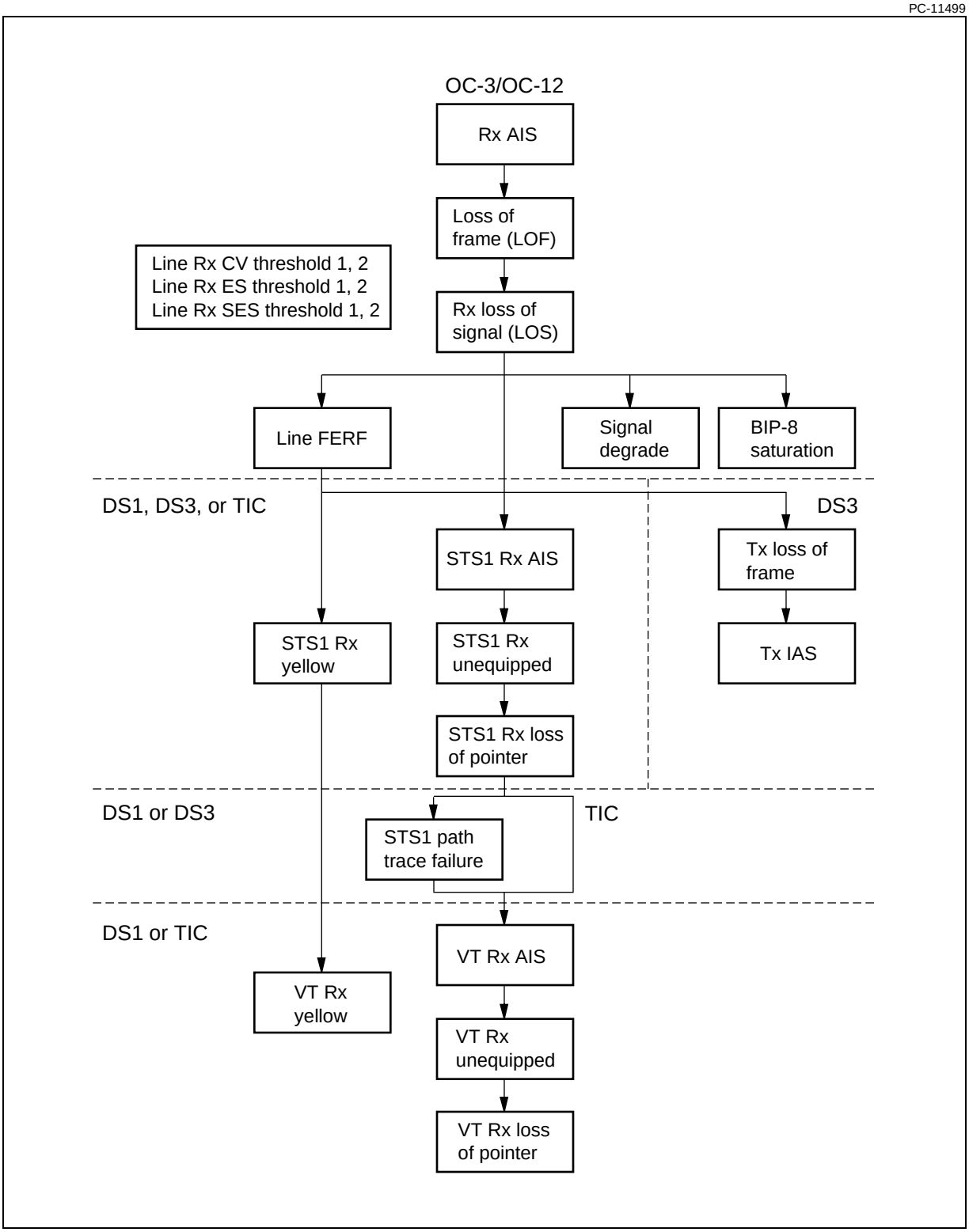


Figure 2-2 (part 2 of 3)
Facility alarm hierarchies

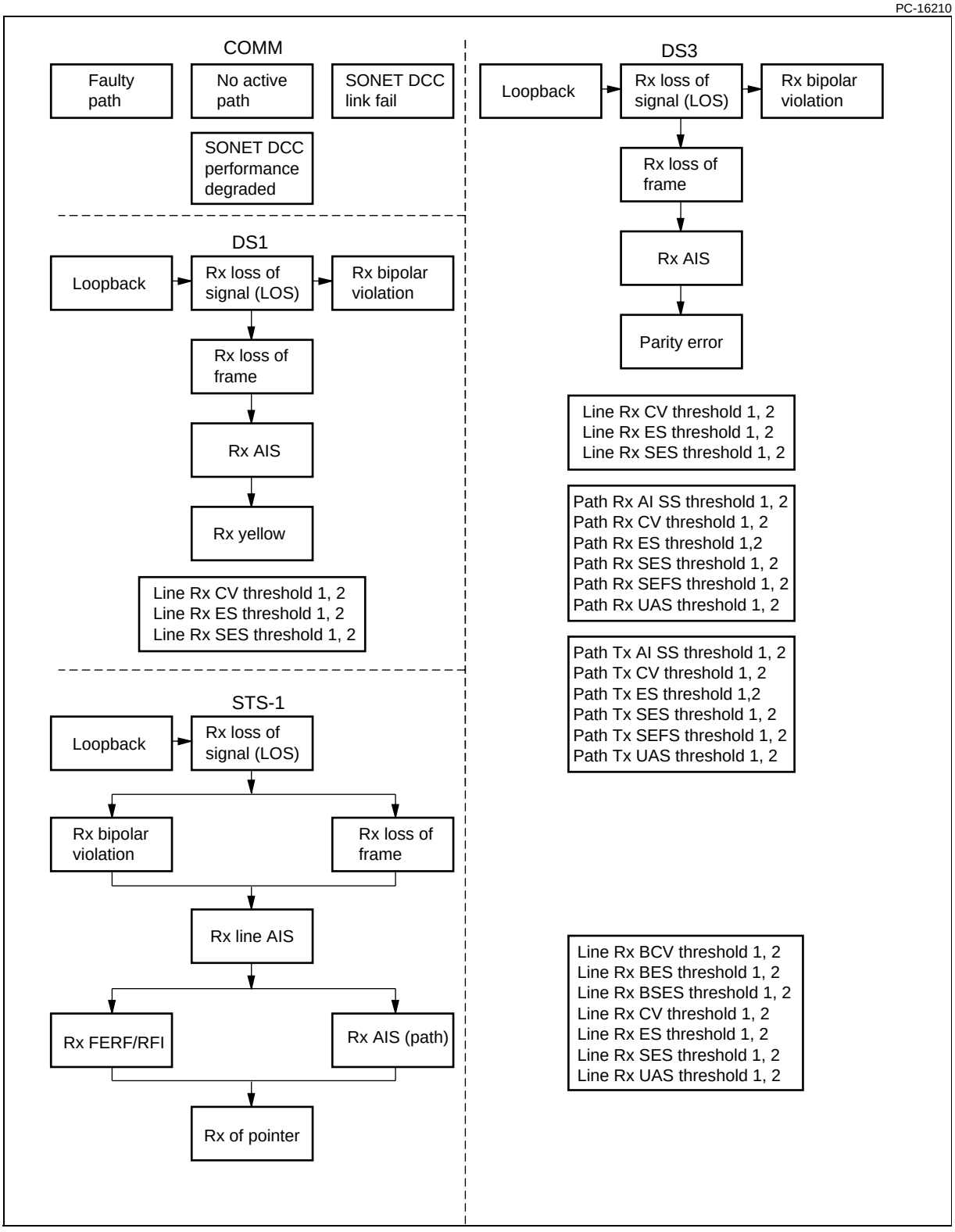
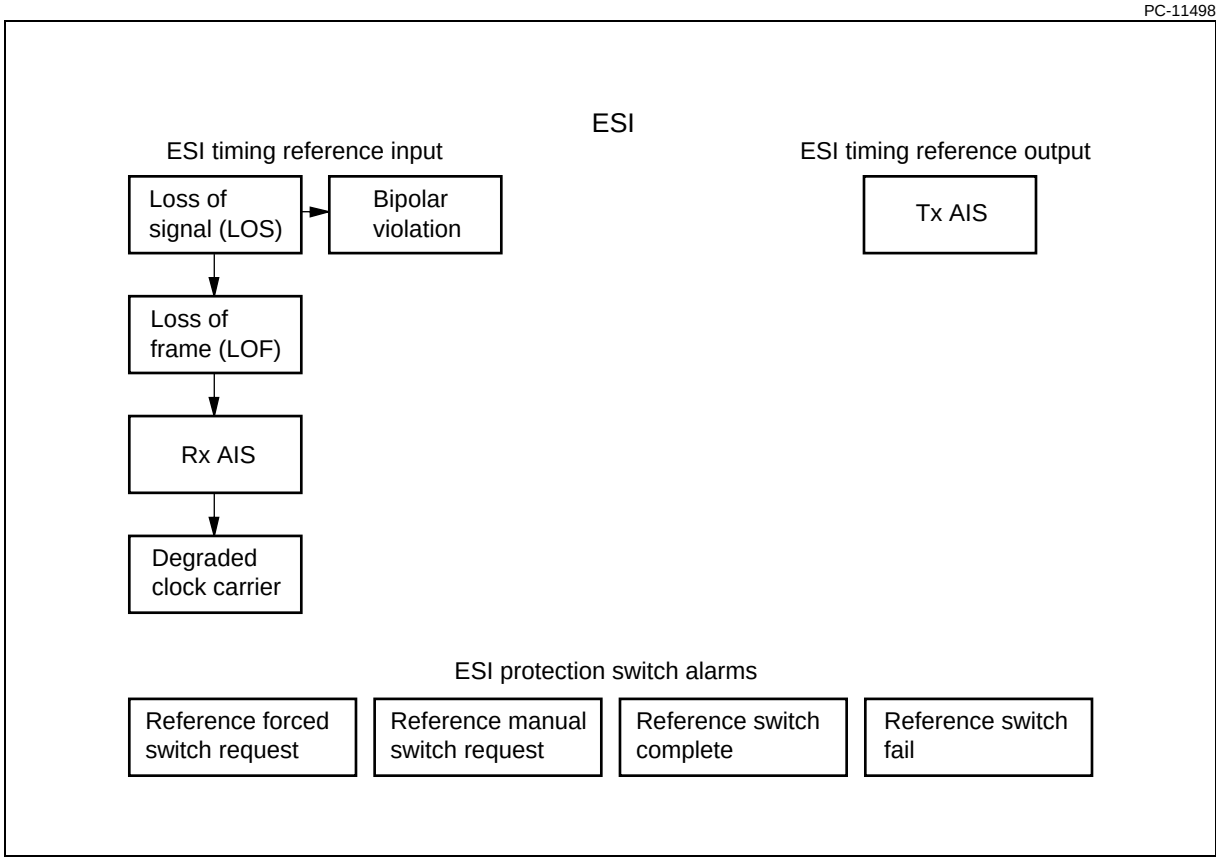


Figure 2-3 (part 3 of 3)
Facility alarm hierarchies



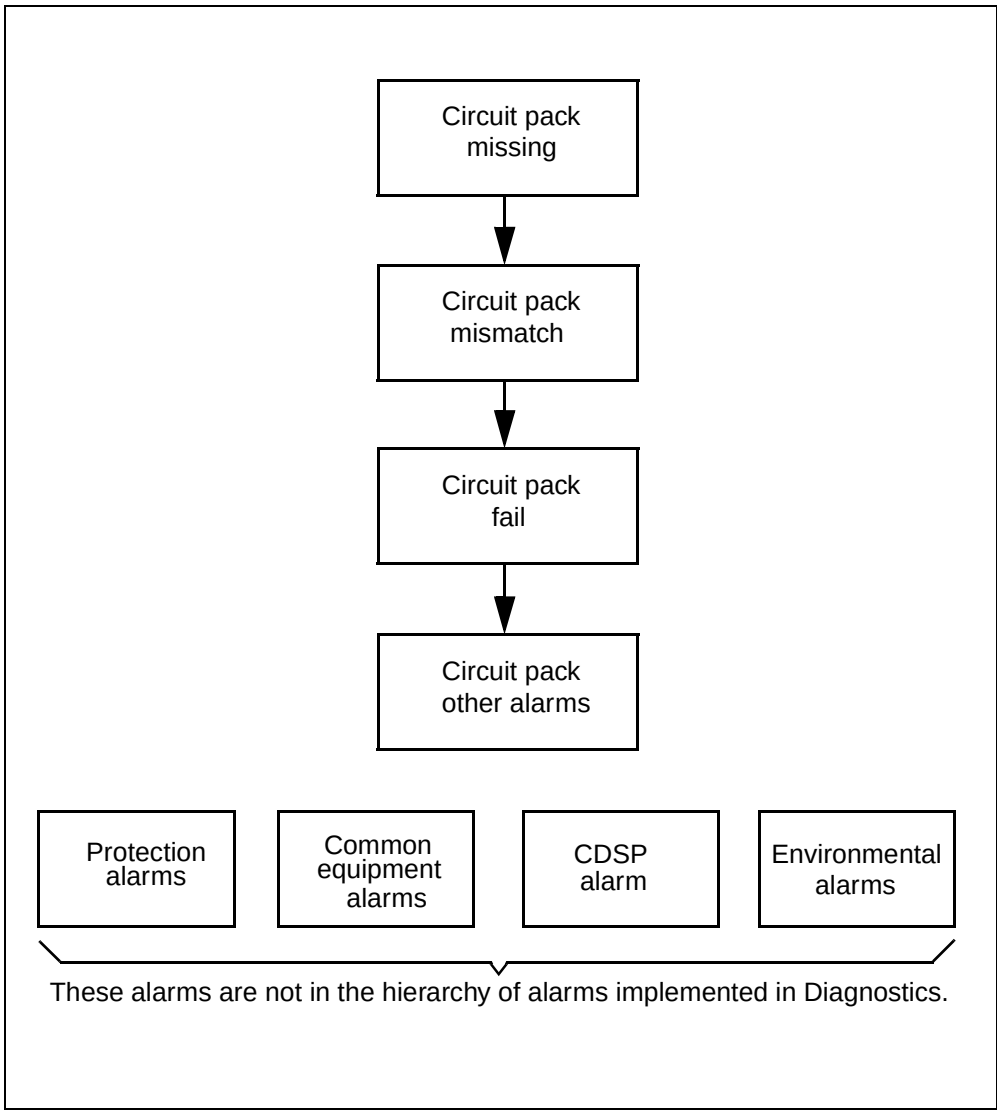
Equipment alarm hierarchy

Equipment alarms identify the nature of a failure and the affected equipment. Figure 2-4 on page 2-6 shows the hierarchy of the three common alarms to all circuit packs (except the processor circuit pack).

As a rule, equipment alarms mask all facility alarms. The following equipment alarms do not mask facility alarms:

- Protection path fail (for DS3 only)
- Switcher circuit pack missing (for DS3 only)

Figure 2-4
Equipment alarm hierarchy



Example of equipment alarms at different levels

Inserting a failed DS1/VT mapper circuit pack by mistake into a slot provisioned for a DS3/STS mapper raises a Circuit pack mismatch alarm. The Circuit pack failure alarm is not raised because it is lower in the hierarchy.

Example of equipment alarms at the same level

The failure of the optical laser and photodetector on an OC-3 or OC-12 optical interface circuit pack raises two alarms: an optical-laser failure alarm and an OC-3 or OC-12 optical interface component failure alarm. Both alarms are raised because the two alarms are on the same level in the hierarchy.

Common equipment alarm hierarchy

The OPC, MIC, and ESI common-equipment circuit packs also use the hierarchy shown in Figure 2-4 on page 2-6.

Example of a common-equipment alarm

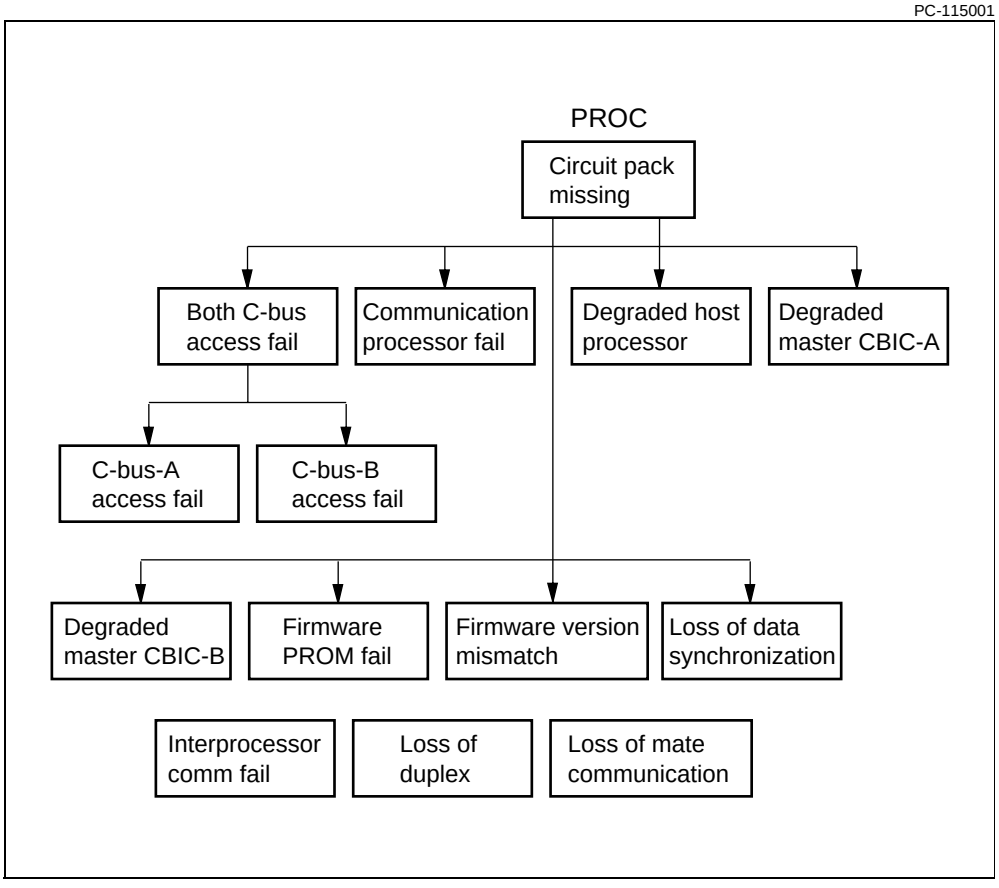
The MIC detects a serial telemetry port failure and raises the Serial telemetry port fail alarm. A failure occurs on the MIC. The MIC Circuit pack fail alarm is generated, and the Serial telemetry port fail alarm disappears because it is masked by the MIC failure alarm.

Proc alarm hierarchy

The processor common-equipment circuit pack (Proc) follows its own alarm hierarchy, which is shown in Figure 2-5.

Figure 2-5
Processor common-equipment alarm hierarchy

PC-115001



Environmental alarm hierarchy

All environmental alarms are on the same level of hierarchy and do not mask each other. Examples of these alarms follow

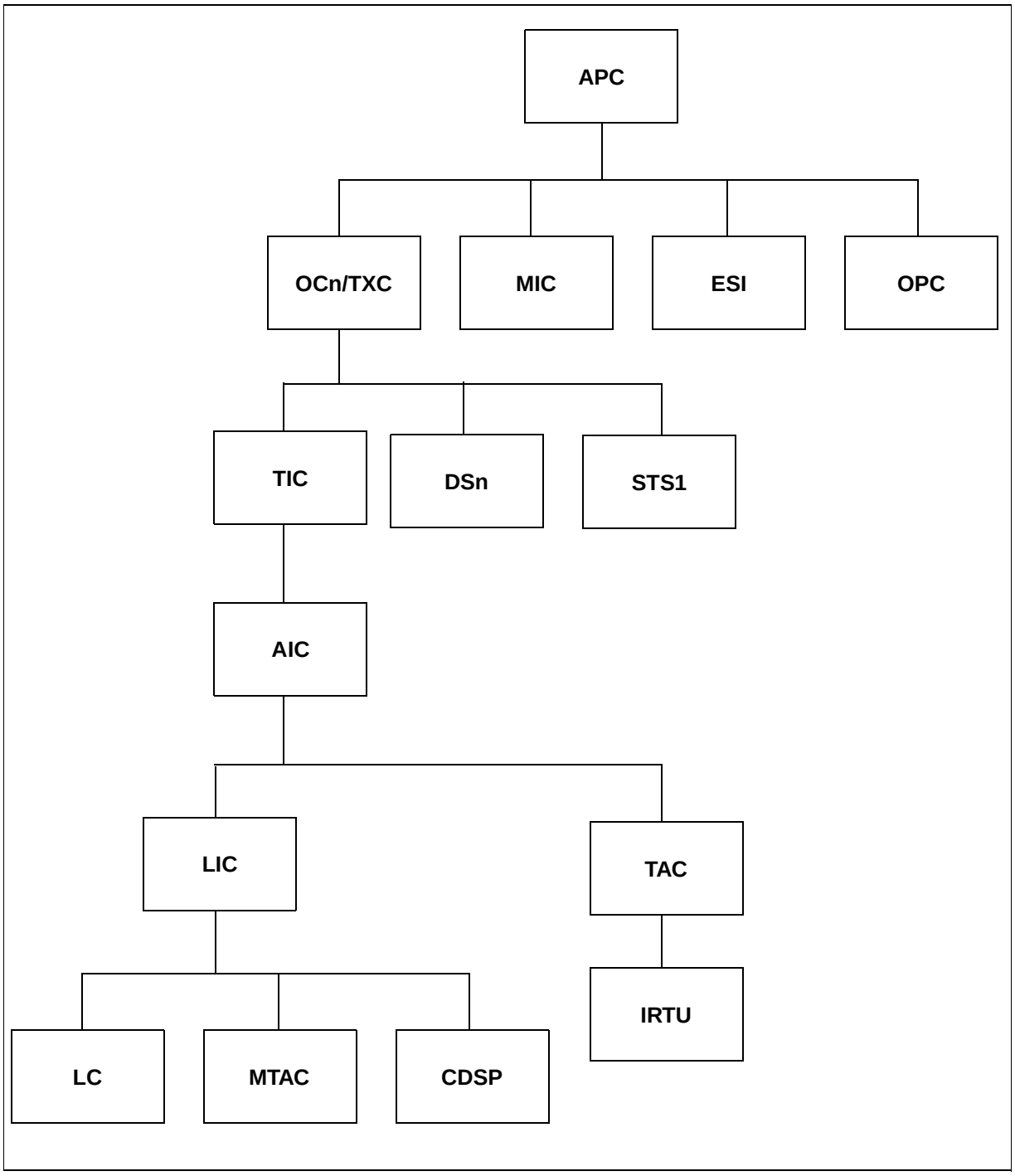
Example of an environmental alarm

An external alarm input (telemetry latch) is activated, but not reported, because the MIC is missing. The telemetry latch alarm is raised as soon as the MIC is inserted in the shelf.

Parent equipment hierarchy

Figure 2-6 on page 2-9 shows the parent equipment hierarchy for AccessNode circuit packs.

Figure 2-6
Parent equipment hierarchy



Clearing an equipment alarm

The procedures in this chapter describe how to clear equipment-class (Eqp) alarms. The alarms appear alphabetically within alarm types (for example, AIC, OC-12, or TXC). The banner at the top of each page shows the alarm type and the text of the alarm. The procedure describes the cause of an alarm and the action needed to clear it.

Chapter contents

The following tables organize equipment class alarms by alarm type. Each table lists the alarms within a type and the page numbers of the alarm procedures.

Note: If you cannot find an alarm in this book, see:

- *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543.
- *UE9000 Voice OAM&P User Guide*

Table 3-1
Eqp AIC alarms

Alarm	See
Circuit pack fail	page 3-20
Circuit pack mismatch	page 3-21
Circuit pack missing	page 3-22
Comm overhead clock/frame loss	page 3-23
Comm overhead data loss	page 3-24
D-link interface fail	page 3-26
Firmware version mismatch	page 3-29
Plane messaging corruption	page 3-30
T-link interface fail	page 3-31

Table 3-2
Eqp ANX alarms

Alarm	See
ANX loss of comms	page 3-33
Circuit pack fail	page 3-33
Circuit pack mismatch	page 3-33
Shelf mismatch	page 3-33
Talk battery failure	page 3-33
Threshold 1 DS0 exceeded	page 3-34
Threshold 2 DS0 exceeded	page 3-34

Table 3-3
Eqp ATM alarms

Alarm	See
Circuit pack fail	page 3-35
Circuit pack missing	page 3-35

Table 3-4
Eqp CDS alarms

Alarm	See
Power filter A missing	page 3-36
Power filter B missing	page 3-39

Table 3-5
Eqp CDSP alarms

Alarm	See
Access failure	page 3-42
Circuit pack fail	page 3-43
Circuit pack mismatch	page 3-44
Circuit pack missing	page 3-45
Clock failure	page 3-46

Table 3-6
Eqp CE alarms

Alarm	See
Autoprovisioning mismatch	page 3-47
Both planes non-operational	page 3-48
CNet link fail	page 3-51
CNet performance degraded	page 3-52
Critical test alarm	page 3-53
Database not restored. Type Q APPROVE at NE	page 3-54
Entry to SONET clock freerun	page 3-56
Exerciser fail	page 3-59
Loss of data synchronization	page 3-60
Major test alarm	page 3-61
Minor test alarm	page 3-62
Plane A non-operational	page 3-63
Plane B non-operational	page 3-65
Ring reconfiguration in progress	page 3-67
Shelf assembly fail	page 3-68
Shelf ID bus fail	page 3-69
Software trap	page 3-70
SONET overhead data/clock loss	page 3-71
—continued—	

Table 3-6 (continued)
Eqp CE alarms

Alarm	See
Timing generation primary reference fail Timing generation secondary reference fail	page 3-73
Traffic upgrade in progress	page 3-77
Warning test alarm	page 3-78
User port 1 intrusion attempt User port 2 intrusion attempt User port 3 intrusion attempt User port 4 intrusion attempt	page 3-79
—end—	

Table 3-7
Eqp DS1 alarms

Alarm	See
Circuit pack fail	page 3-80
Circuit pack mismatch	page 3-81
Circuit pack missing	page 3-83
Facility provisioning mismatch	page 3-84
Forced switch request	page 3-85
Input card fail -DoNotRemove	page 3-86
Input card mismatch	page 3-87
Input card missing	page 3-88
Lockout request	page 3-89
Manual switch request	page 3-90
Output card fail - DoNotRemove	page 3-91
Output card mismatch	page 3-92
Output card missing	page 3-93
Prot bridge in card fail -DoNotRemove	page 3-94
Prot bridge in card mismatch	page 3-95
Prot bridge in card missing	page 3-96
—continued—	

Table 3-7 (continued)
Eqp DS1 alarms

Alarm	See
Prot bridge out card fail -DoNotRemove	3-97
Prot bridge out card mismatch	3-98
Prot bridge out card missing	3-99
Protection path fail	3-101
Protection switch complete	3-105
Protection switch fail	3-106
Protection version mismatch	3-110
STS1 intercard fail	3-111
—end—	

Table 3-8
Eqp DS3 alarms

Alarm	See
BNC I/O card 1 fail -DoNotRemove, BNC I/O card 2 fail -DoNotRemove, BNC I/O card 3 fail -DoNotRemove	3-112
BNC I/O card 1 mismatch, BNC I/O card 2 mismatch, BNC I/O card 3 mismatch	3-113
BNC I/O card 1 missing, BNC I/O card 2 missing, BNC I/O card 3 missing	3-114
Circuit pack fail	3-115
Circuit pack mismatch	3-116
Circuit pack missing	3-117
Forced switch	3-118
Lockout request	3-119
Manual switch request	3-120
Protection path fail	3-121
—continued—	

Table 3-8 (continued)
Eqp DS3 alarms

Alarm	See
Protection switch complete	3-124
Protection switch fail	3-126
STS1 intercard fail	3-129
Switcher circuit pack mismatch	3-131
Switcher circuit pack missing	3-132
Traffic problem detected	3-133
VT connection provisioning mismatch	page 3-136
—end—	

Table 3-9
Eqp DTAP alarms

Alarm	See
Circuit pack fail	3-137
Circuit pack mismatch	3-138
Circuit pack missing	3-139
Circuit pack partial fail	3-140

Table 3-10
Eqp ESI alarms

Alarm	See
End VCO range	3-141
Equipment forced switch request	3-142
Equipment lockout request	3-143
Equipment manual switch request	3-144
Equipment protection switch complete	3-145
Equipment protection switch fail	3-146
Failure to lock	3-147
Intercard failure	3-148
Subunit fail	3-149
—continued—	

Table 3-10 (continued)
Eqp ESI alarms

Alarm	See
Subunit mismatch	3-150
Subunit missing	3-151
Timing generation entry to acquire	3-152
Timing generation entry to fast	3-153
Timing generation entry to freerun	3-154
Timing generation entry to holdover	3-156
—end—	

Table 3-11
Eqp IRTU alarms

Alarm	See
Circuit pack fail	3-158
Circuit pack mismatch	3-159
Circuit pack missing	3-160
Common circuitry fail	3-161
Software download fail	3-163
Test head 1 fail	3-165
Test head 2 fail	3-167

Table 3-12
Eqp ITU alarms

Alarm	See
Circuit pack fail	page 3-169
Circuit pack mismatch	page 3-169
Circuit pack missing	page 3-169

Table 3-13
Eqp LC alarms

Alarm	See
Line card fail	3-170
Line card missing	3-177
Loss of power at NT1	3-178
NT1 power status changed	3-179
NT1 test mode changed	3-180
Sync lost with NT1	3-181

Table 3-14
Eqp LIC alarms

Alarm	See
A-link clock driver fail	3-182
Circuit pack fail	3-184
Circuit pack mismatch	3-187
Circuit pack missing	3-188
D-link interface fail	3-190
Inter-plane fail	3-196
Plane messaging corruption	page 3-198

Table 3-15
Eqp MIC alarms

Alarm	See
Alarm relay fail	3-201
Circuit pack fail	3-202
Circuit pack mismatch	3-203
Circuit pack missing	3-204
E2A input fail	3-205
Firmware version mismatch	3-206
LED driver fail	3-209
Local craft interface port fail	3-210
—continued—	

Table 3-15 (continued)
Eqp MIC alarms

Alarm	See
Non-volatile store fail	3-211
Non-volatile store mismatch	3-212
Orderwire fail	3-213
Parallel telemetry relay fail	3-214
Performance monitor clock fail	3-215
Protection switch relay fail	3-216
Serial telemetry port fail	3-217
Time of day clock fail	3-218
—end—	

Table 3-16
Eqp MLC alarms

Alarm	See
Circuit pack fail	page 3-219
Circuit pack mismatch	page 3-219
Circuit pack missing	page 3-219
Partial circuit pack fail	page 3-219

Table 3-17
Eqp MTAC alarms

Alarm	See
Circuit pack fail	3-220
Circuit pack mismatch	3-221
Circuit pack missing	3-222

Table 3-18
Eqp OC1 alarms

Alarm	See
Rx line AIS Rx loss of frame Rx loss of signal Rx RFI Rx signal degrade Rx signal failure Rx section trace mismatch	page 3-223
STS1 Rx AIS STS1 Rx excessive BIP error rate STS1 Rx loss of pointer STS1 Rx path trace mismatch STS1 Rx RFI STS1 Rx signal degrade STS1 Rx signal label mismatch STS1 Rx unequipped	page 3-224
VT Rx AIS VT Rx excessive BIP error rate VT Rx loss of pointer VT Rx RFI VT Rx signal degrade VT Rx signal label mismatch VT Rx unequipped	page 3-225

Table 3-19
Eqp OC-3/OC-12 alarms

Alarm	See
Channel match fail	3-226
Circuit pack fail	3-227
Circuit pack mismatch	3-228
Circuit pack missing	3-229
Circuit pack reach mismatch	3-230
Entry to SONET clock freerun	page 3-231
Fiber connection error	3-233
Firmware version mismatch	3-234
Forced switch request	3-235
—continued—	

Table 3-19 (continued)
Eqp OC-3/OC-12 alarms

Alarm	See
Intercard failure	3-236
Laser bias current	3-239
Laser degrade	3-240
Lockout protection operation fail	page 3-241
Lockout request	3-242
Manual switch request	3-243
Protection oscillation control activated	3-244
Protection path fail	3-245
Protection scheme mismatch	3-247
Protection switch complete	3-248
Protection switch fail	3-249
Protection switching byte fail/Improper APS code	3-251
Receive fail	3-252
STS1 intercard fail	3-253
Switch mode mismatch	3-255
Transmission rate mismatch	3-257
Transmit fail	3-258
Unable to track clock reference	3-259
—end—	

Table 3-20
Eqp OC-12 alarms

Alarm	See
Default K bytes	page 3-260
Duplicate NE ID Alarm	page 3-261
Duplicate NE Name	page 3-262
Entry to SONET clock acquire	page 3-264
Entry to SONET clock freerun	page 3-265
—continued—	

Table 3-20 (continued)
Eqp OC-12 alarms

Alarm	See
Entry to SONET clock holdover	page 3-266
Fiber loopback	3-268
Firmware corrupt	3-269
Firmware/software incompatible	3-270
Firmware trap	3-271
Intercard serial link fail	3-272
Invalid neighbor detected	page 3-273
Lockout protection request	page 3-275
Lockout working request	page 3-276
Maps invalid	3-277
Matchnode connection provisioning mismatch	3-278
NE id mismatch	3-279
Performance monitor clock fail	3-280
Protection switching byte/APS code inconsistent	3-281
Reference input clock fail	3-282
Ring protection suspended or unavailable	page 3-283
STS1 intercard fail	3-284
STS12 ring link parity error	3-285
Synchronization clock fail	3-286
System clock reference fail	3-287
VT connection provisioning mismatch	3-288
—end—	

Table 3-21
Eqp OPC alarms

Alarm	See
Configuration audit fail	page 3-289
Connection audit fail	page 3-291
Datasync fail	3-293
Lost peer OPC	3-294
NE DB missing/outdated	page 3-295
OPC alarm(s) active	page 3-297
OPC circuit pack fail	3-298
OPC circuit pack mismatch	3-299
OPC circuit pack missing	3-300
OPC CNET loss of signal	3-301
OPC Ethernet loss of signal	3-302
OPC hardware reset	3-305
OPC OAM software fail	3-306
OPC serial I/O card mismatch	3-307
OPC serial I/O card missing	3-308
Tape backup/Restore fail	3-309

Table 3-22
Eqp Proc alarms

Alarm	See
Both C-bus access fail	3-312
C-bus-A access fail	3-313
C-bus-B access fail	3-314
Circuit pack missing	3-315
Communication processor fail	3-316
Degraded communication processor	3-317
Degraded host processor	3-318
Degraded master CBIC-A	3-319
—continued—	

Table 3-22 (continued)
Eqp Proc alarms

Alarm	See
Degraded master CBIC-B	3-320
Firmware PROM Fail	3-321
Interprocessor comm fail	3-322
Loss of data synchronization	3-323
Loss of duplex	3-324
Loss of mate communication	3-325
—end—	

Table 3-23
Eqp PSU alarms

Alarm	See
Circuit pack fail	page 3-326
Circuit pack mismatch	3-326
Circuit pack missing	3-326

Table 3-24
Eqp SI alarms

Alarm	See
Circuit pack fail	page 3-327
Circuit pack mismatch	page 3-327
Circuit pack missing	page 3-327
Signal battery A loss	page 3-327
Signal battery B loss	page 3-327
Talk battery A loss	page 3-327
Talk battery B loss	page 3-327

Table 3-25
Eqp SPX alarms

Alarm	See
Circuit pack fail	page 3-328
Circuit pack mismatch	page 3-328
Circuit pack missing	page 3-328
Duplex SP comms failure	page 3-328
Environmental alarm hw fail	page 3-328
ITU comms failure	page 3-328
ITU datasync fail	page 3-328
Loss of primary timing reference	page 3-329
Loss of secondary timing reference	page 3-329
SID mismatch	page 3-329
Software release mismatch	page 3-329
SP datasync fail	page 3-329
Timing generation entry to freerun	page 3-329
Upgrade in progress	page 3-329

Table 3-26
Eqp STS1 alarms

Alarm	See
BNC I/O card 1 fail BNC I/O card 2 fail BNC I/O card 3 fail	page 3-330
BNC I/O card 1 mismatch BNC I/O card 2 mismatch BNC I/O card 3 mismatch	page 3-331
BNC I/O card 1 missing BNC I/O card 2 missing BNC I/O card 3 missing	page 3-332
Circuit pack fail	page 3-333
Circuit pack mismatch	page 3-334
Circuit pack missing	page 3-335
—continued—	

Table 3-26 (continued)
Eqp STS1 alarms

Alarm	See
Firmware failure	page 3-336
Firmware/software incompatible	3-337
Forced switch request	page 3-338
Lockout request	page 3-339
Manual switch request	page 3-340
Protection path fail	page 3-341
Protection switch complete	page 3-344
Protection switch fail	page 3-345
STS1 intercard fail	3-347
Switcher circuit pack mismatch	page 3-348
Switcher circuit pack missing	page 3-349
Traffic problem detected	page 3-350
VT connection provisioning mismatch	page 3-353
—end—	

Table 3-27
Eqp TAC alarms

Alarm	See
Circuit pack fail	3-354
Circuit pack mismatch	3-355
Circuit pack missing	3-356
Digital side fail	3-357
Metallic side fail	3-358
PGTC I/O card mismatch	3-359
Software download fail	3-360
TAP I/O card mismatch	3-362
TBP I/O card mismatch	3-363

Table 3-28
Eqp TDM alarms

Alarm	See
A-link clock driver fail	page 3-364
Circuit pack fail	page 3-364
Circuit pack mismatch	page 3-364
Circuit pack missing	page 3-364
Control link fail to TDM-A	page 3-364
Control link fail to TDM-B	page 3-364
D-link interface fail	page 3-365
Loss of mate communication	page 3-365
PCM path fail to TDM-A	page 3-365
PCM path fail to TDM-B	page 3-365
TDM inter-plane fail	page 3-365

Table 3-29
Eqp TIC alarms

Alarm	See
Backplane parity error	3-366
Circuit pack fail	3-367
Circuit pack mismatch	3-368
Circuit pack missing	3-369
Loss of signal synchronization	3-370
T-link interface fail	3-371
TR-08 circuit pack mismatch	3-373

Table 3-30
Eqp TXC alarms

Alarm	See
Circuit pack failure	3-374
Circuit pack mismatch	3-375
Circuit pack missing	3-376
End VCO range	3-377
Equipment lockout request	3-378
Equipment protection switch complete	3-379
Equipment protection switch fail	3-380
Equipment prot oscillation control activated	3-382
Failure to lock	3-383
Forced equipment switch request	3-385
Forced timing reference switch request	3-386
Intercard: STS1 parity error or clock fail	3-387
Manual equipment switch request	3-389
Manual timing reference switch request	3-390
Partial circuit pack fail	3-391
Serial link failure	3-392
Sys clock src entry to freerun	3-393
—continued—	

Table 3-30 (continued)
Eqp TXC alarms

Alarm	See
Timing gen entry to acquire mode	3-395
Timing gen entry to fast mode	3-396
Timing gen entry to freerun mode	3-397
Timing gen entry to holdover mode	3-400
Timing generation primary reference fail	3-401
Timing generation secondary reference fail	3-403
Timing ref lockout request	3-405
Timing ref prot oscillation control activated	page 3-406
Timing ref prot switch complete	3-407
Timing ref prot switch fail	page 3-408
—end—	

Table 3-31
Eqp UE alarms

Alarm	See
TDM firmware mismatch	page 3-409
Upgrade in progress	page 3-409

Eqp AIC
Circuit pack fail

Probable cause

The access interface card failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp AIC
Circuit pack mismatch

Probable cause

The circuit pack in the slot designated for the access interface card does not match the provisioned circuit pack. This alarm can also be caused by an AIC with an incorrect vintage.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, and correct vintage, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp AIC
Circuit pack missing

Probable cause

The access interface card is missing from its designated slot.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

If the circuit pack is present in the slot, ensure that it is properly seated.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp AIC
Comm overhead clock/frame loss

Probable cause

The system has detected a clock/frame loss on the communication overhead bus, due to a faulty AIC or a faulty processor card.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action

1 Replace the AIC against which this alarm is raised. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end the procedure
persists	go to step 2

2 Replace the redundant (standby) processor. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end the procedure
persists	go to step 3

3 Replace the primary (active) processor. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end the procedure
persists	if you cannot successfully complete this procedure, contact your next level of support

—end—

Eqp AIC
Comm overhead data loss

Probable cause

The system has detected a parity error on the communication overhead bus, due to a faulty AIC or TIC, or a faulty processor card.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action

1 Replace the AIC against which this alarm is raised. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end the procedure
persists	go to step 2

2 Replace the TIC that resides on the same plane as the AIC in step 1. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end the procedure
persists	go to step 3

—continued—

Eqp AIC
Comm overhead data loss (continued)

Step	Action
3	Replace the redundant (standby) processor, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end the procedure
persists	go to step 4

Step	Action
4	Replace the primary (active) processor as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end the procedure
persists	if you cannot successfully complete this procedure, contact your next level of support

—end—

Eqp AIC
D-link interface fail

Probable cause

The system has detected a failure on the D-link between the access interface card (AIC) and the line interface card (LIC). The corresponding LIC will have the same alarm raised with a warning severity. The fault can be due to a faulty AIC, D-link cable, or LIC.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

If the severity of this alarm is warning, not service-affecting (w, nsa), the problem is most likely associated with the card at the other end of the link.

Action

Step	Action
1	Determine the severity of the alarm.

If the severity of this alarm is	Then
C, SA	go to step 2
m, nsa	go to step 2
w, nsa	go to step 6

2 Determine the LIC and D/VT link access cable that are associated with this alarm as follows:

a. From any FWPUI screen, display the list of active alarms:

alarms↵

The list of active alarms appears.

—continued—

Eqp AIC
D-link interface fail (continued)

Step	Action

b. Identify from the list of active alarms, the D-link interface fail alarm raised against the LIC, and display the detailed alarm report:

dtlalms < alarm # >↵

where

< alarm # >	the alarm report number displayed on screen

The detailed alarm screen appears, showing the shelf and slot number of the LIC.

c. Record the LIC shelf, unit, location, and slot information.

d. Determine the D/VT link access cable (NT4K82) associated with this alarm.

Note: The AIC in slot 13 on the common-equipment (CE) shelf is associated with plane A, and is connected by D-links to LIC A and C on each CDS. The AIC in slot 16 is associated with plane B, and is connected by D-links to LIC B and D on each CDS. Fourteen D/VT link access cables (NT4K82) carry the D-links between the CE shelf and the seven CDS. There are two D/VT link access cables for each CDS. One cable carries the D-links for the two LICs in plane A on the CDS, and the second cable carries the D-links for the two LICs in plane B.
For example, the external D/VT link access cable that connects the AIC in slot 13 with LIC C on CDS 2, attaches to connector “CDS A” on CDS shelf 2, and attaches to connector “CDS 2A” on the side interconnect right.

3 Reseat the D/VT link access cable (identified in step 2) on its connectors at the CDS and side interconnect right circuit pack.

If this alarm	Then
clears	end the procedure
persists	go to step 4

4 Replace the AIC against which this alarm is raised, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end of procedure
persists	a. Re-insert the AIC that you replaced earlier in this step. b. Replace the LIC that you identified in step 2, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C. Go to step 5.

—continued—

Eqp AIC
D-link interface fail (continued)

Step	Action

5 Determine if this alarm clears.

If this alarm	Then
clears	end the procedure
persists	a. Re-insert the LIC that you replaced in step 4. b. Replace the D/VT link access cable that you identified in step 2. For details see *Bay in a Central Office Installation for ABM,* 323-3001-201. End the procedure.

6 From any FWPUI screen, display the list of active alarms:

alarms↵

The list of active alarms appears.

7 Identify from the list of active alarms, the **D-link interface fail** alarm raised against the LIC, and display the detailed alarm report:

dtlalms < alarm # >↵

where

< alarm # >	the alarm report number displayed on screen

The detailed alarm screen appears, showing the shelf and slot number of the LIC.

8 Replace the LIC identified in the step 7 as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

9 If the alarm persists, replace the AIC against which this alarm was originally raised. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

10 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp AIC
Firmware version mismatch

Probable cause

The software release on the loopback access interface (LAIC) circuit card is not the latest software release supported by the access processing unit (APU) circuit card.

CAUTION
Loss of service
If the software release on the HDT is upgraded without first upgrading the LAIC circuit card software, the HDT and LAIC will be incompatible. All traffic on the HDT is dropped.

You must upgrade the LAIC circuit card software to the latest software release before you upgrade the host digital terminal (HDT) software. If you do not upgrade the LAIC circuit card before upgrading the HDT, all traffic on the HDT will be lost.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Upgrade the indicated LAIC circuit card with the latest software release. See *AccessNode Express Commissioning and OAM&P*, 323-3051-220, in the *AccessNode Express* volume for details on upgrading the LAIC circuit card software.

—end—

Eqp AIC
Plane messaging corruption

Probable cause

Line cards detected cyclic redundancy check (CRC) errors in all of the drawers of one plane.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

If the severity of this alarm is warning, not service-affecting (w, nsa), the line cards detected the CRC errors in some, rather than all, of the drawers in one plane.

Action

Step	Action
1	From any FWPUI screen display the list of active alarms by entering: **alarms**↵ *The list of active alarms appears.*
2	Identify the alarm against the line interface card (LIC), then display the alarm report by entering: **dtlalms < alarm # >**↵ where < alarm # > the alarm report number displayed on screen *The detailed alarm screen displays the shelf and slot number of the LIC.*
3	Replace the LIC. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If the alarm	Then
clears	end the procedure
persists	contact your next level of support

—end—

Eqp AIC
T-link interface fail

Probable cause

The system has detected a failure on the T-link between the access interface card (AIC) and the transport interface card (TIC).

Note: This same alarm is also raised as an equipment alarm against the corresponding TIC.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

If the severity of this alarm is warning, not service-affecting (w, nsa), the problem is most likely associated with the card at the other end of the link.

Action

Step	Action

If the severity of this alarm is	Then
C, SA	go to step 1
m, nsa	go to step 1
w, nsa	go to step 2

1 Replace the AIC against which this alarm is raised. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end the procedure
persists	go to step 2

2 From any FWPUI screen, display the list of active alarms:

alarms.↵

The list of active alarm appears.

—continued—

Eqp AIC
T-link interface fail (continued)

Step	Action
3	Identify from the list of active alarms, the **T-link interface fail** alarm raised against the TIC, and display the detailed alarm report: **dtlalms < alarm # >**↵ where < alarm # > the alarm report number displayed on screen *The detailed alarm screen appears, showing the shelf and slot number of the card.*
4	Replace the TIC identified in the previous step. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
5	If the alarm persists, replace the AIC against which this alarm was originally raised. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ANX
ANX loss of comms
Circuit pack fail
Circuit pack mismatch
Shelf mismatch
Talk battery failure

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543 for information on the following AccessNode Express alarms and the appropriate alarm clearing procedures.

The following alarm is an AccessNode Express DS1 facility alarm.

- HDT comms failure (ANX loss of comms)

The following alarms are AccessNode Express HDSL shelf processor circuit card alarms.

- Circuit pack fail
- Circuit pack mismatch
- HDT denies connection - shelf mismatch (Shelf mismatch)

The following alarm is an AccessNode Express talk battery filter circuit card alarm.

- Talk battery failure

—end—

Eqp ANX
Threshold 1 DS0 exceeded
Threshold 2 DS0 exceeded

Probable cause

The user provisioned threshold for traffic channel usage between the host digital terminal (HDT) and the AccessNode Express voice module (VM) has been crossed.

Note: For information on provisioning traffic thresholds and on traffic monitoring, see *AccessNode Express Commissioning and OAM&P*, 323-3051-220, in the *AccessNode Express* volume.

Impact

For the threshold 1 alarm, this is a warning, not service-affecting (w, nsa) or minor, not service-affecting (m, nsa) alarm.

For the threshold 2 alarm, this is a minor, not service-affecting (m, nsa) or major, not service-affecting (M, nsa) alarm.

Action

Step	Action
1	Add one or more DS1 facilities between the HDT and the VM.

—end—

Eqp ATM
Circuit pack fail
Circuit pack missing

See the *UE9000 Voice OAM&P Guide* for information on the following Universal Edge 9000 (UE9000) alarms and the appropriate alarm clearing procedures.

The following alarms are associated with the asynchronous transfer mode (ATM) card on the UE9000 shelf:

- Circuit pack fail
- Circuit pack missing

—end—

Eqp CDS
Power filter A missing

Probable cause

The NT4K63AA power filter card has been removed from the left hand drawer of the copper-distribution shelf (CDS).

> ***Note:*** It may take up to one minute for this alarm to be raised after the power filter card is removed from the drawer.

Impact

This is a minor, service-affecting (m, SA) alarm.

Since the function of the power filter card is to provide filtering for the DC power supplied to the line cards, there may be noise-related problems reported on the lines in the affected drawer.

Action

Step	Action
1	From the alarm text, identify the affected copper-distribution shelf number.
2	From the Network Element Status screen access the System Monitor tool at the command interpreter level: **quit all;sysmon**↵ *The System Monitor CI prompt appears.*
3	Obtain a list of in service line cards in the CDS you are working on and record this information: **lcstats shelf <shelf #>**↵ where <shelf #> is the shelf number (**1** to **7**) identified in step 1 *A list of all line cards in the specified CDS shelf are displayed.*

—continued—

Eqp CDS
Power filter A missing (continued)

Step	Action

CAUTION
Loss of service
In the next step, service will be lost to all line cards housed in both drawers of the copper-distribution shelf that is reporting this alarm.

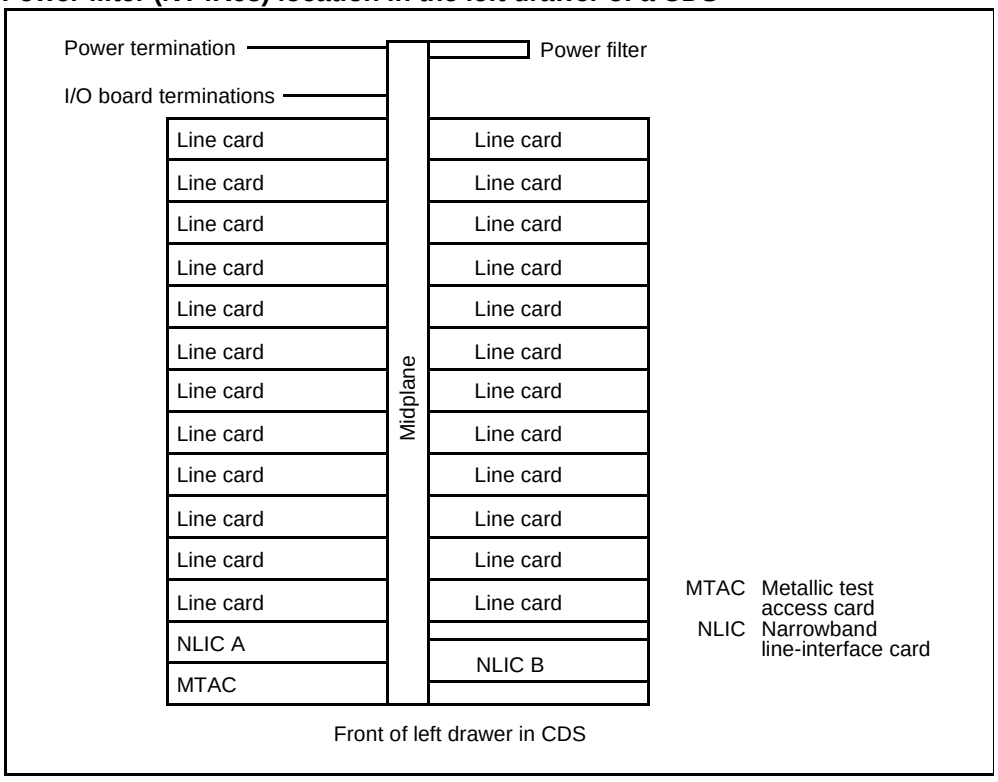
4 At the network element breaker interface panel (BIP), power down the affected copper-distribution shelf by turning off the CDS Power breaker and the Talk Battery breaker for the affected copper-distribution shelf.

Service is lost to all line cards housed in the affected copper-distribution shelf.

5 Unlatch and open the left line card drawer.

Note: Depress the catches on the top and bottom of the drawer so that it slides out far enough to give access to the power filter. The power filter plugs into the midplane at the back of the drawer (on the side of the drawer closest to the center of the shelf).

Figure 3-1
Power filter (NT4K63) location in the left drawer of a CDS



—continued—

Eqp CDS
Power filter A missing (continued)

Step	Action
6	Insert an NT4K63AA power filter card into the rear most slot on the right side of the drawer as shown in Figure 3-1 on 3-37.
7	At the BIP, power up the copper-distribution shelf by turning on the CDS Power breaker and the Talk Battery breaker for the affected copper-distribution shelf. *The system initiates a restart sequence for the copper-distribution shelf, which may take up to five minutes.*
8	Check network element user interface to see that this alarm clears.
9	Verify that there is dial tone to the CDS.
10	Repeat step 3 to verify that the line cards in the CDS you are working on have returned to service.
11	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CDS
Power filter B missing

Probable cause

The NT4K63AA power filter card has been removed from the right hand drawer of the copper-distribution shelf.

Note: It may take up to one minute for this alarm to be raised after the power filter card is removed from the drawer.

Impact

This is a minor, service-affecting (m, SA) alarm.

Since the function of the power filter card is to provide filtering for the DC power supplied to the line cards, there may be noise-related problems reported on the lines in the affected drawer.

Action

Step	Action
1	From the alarm text, identify the affected copper-distribution shelf number.
2	From the network element status screen access the System Monitor tool at the command interpreter level: **quit all;sysmon**↵ *The System Monitor CI prompt appears.*
3	Obtain a list of in service line cards in the CDS you are working on and record this information: **lcstats shelf <shelf #>**↵ where <shelf #> is the shelf number (**1** to **7**) identified in step 1 *A list of all line cards in the specified CDS shelf are displayed.*

—continued—

Eqp CDS
Power filter B missing (continued)

Step	Action

CAUTION
Loss of service
In the next step, service will be lost to all line cards housed in both drawers of the copper-distribution shelf that is reporting this alarm.

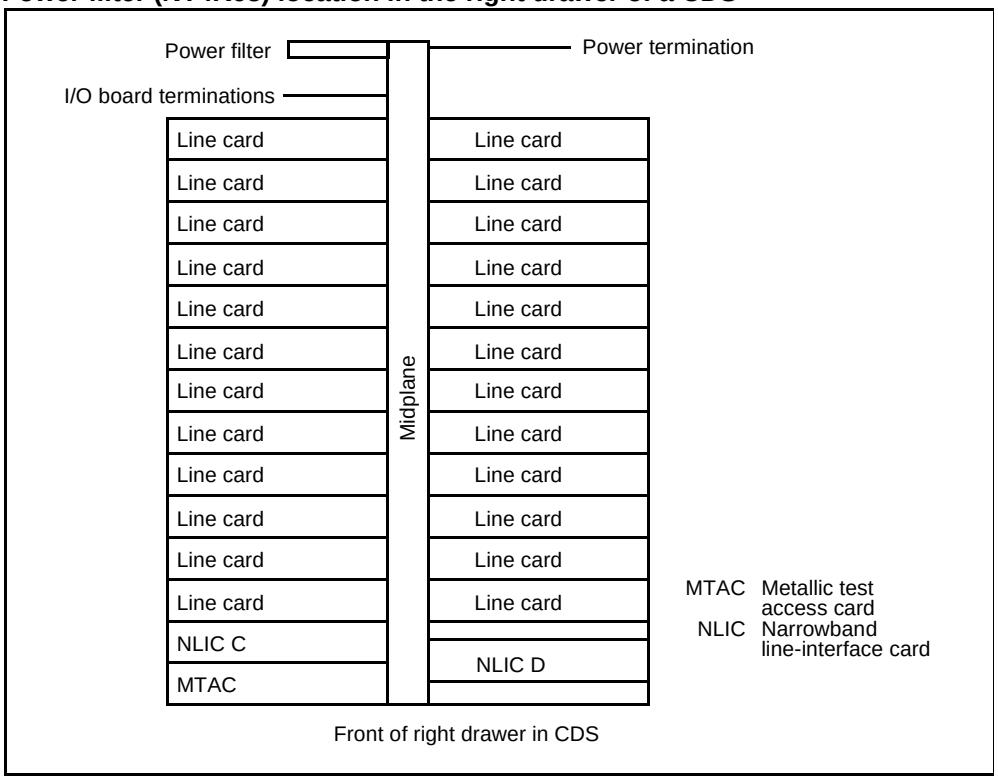
4 At the network element breaker interface panel (BIP), power down the affected copper-distribution shelf by turning off the CDS Power breaker and the Talk Battery breaker for the affected copper-distribution shelf.

Service is lost to all line cards housed in the affected copper-distribution shelf.

5 Unlatch and open the left line card drawer.

Note: Depress the catches on the top and bottom of the drawer so that it slides out far enough to give access to the power filter. The power filter plugs into the midplane at the back of the drawer (on the side of the drawer closest to the center of the shelf).

Figure 3-2
Power filter (NT4K63) location in the right drawer of a CDS



—continued—

Eqp CDS
Power filter B missing (continued)

Step	Action
6	Insert an NT4K63AA power filter card into the rear most slot on the left side of the drawer as shown in Figure 3-2 on page 3-40.
7	At the BIP, power up the copper-distribution shelf by turning on the CDS Power breaker and the Talk Battery breaker for the affected copper-distribution shelf. *The system initiates a restart sequence for the copper-distribution shelf, which may take up to five minutes.*
8	Check network element user interface to see that this alarm clears.
9	Verify that there is dial tone to the CDS.
10	Repeat step 3 to verify that the line cards in the CDS you are working on have returned to service.
11	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CDSP
Access failure

Probable cause

The copper-distribution shelf power converter (CDSP) has detected a problem with the message flow from the access interface card (AIC) and line interface card (LIC) through to the CDSP.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action

Replacing the CDSP

1 Replace the CDSP that raised this alarm, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end the procedure
persists	go to step 2

2 One at a time, replace each line interface card until this alarm clears. Start with NLIC-A and NLIC-B in line drawer A, then NLIC-C and NLIC-D in line drawer B. LIC replacement procedures can be found in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

3 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CDSP
Circuit pack fail

Probable cause

The copper-distribution shelf power converter failed.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CDSP
Circuit pack mismatch

Probable cause

The circuit pack in the slot designated for the copper-distribution shelf power converter does not match the provisioned circuit pack. This alarm can also be caused by a CDSP with an incorrect vintage.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, and correct vintage, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CDSP
Circuit pack missing

Probable cause

The copper-distribution shelf power converter is missing from its designated slot.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

If the circuit pack is present in the slot, ensure that it is properly seated.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If the circuit pack is properly installed, and this alarm is raised, replace the CDSP circuit pack as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If the slot is intentionally empty, clear the alarm by taking the CDSP out-of-service and delete the CDSP to prevent the alarm from being raised again.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CDSP
Clock failure

Probable cause

The clock source from the line interface card (LIC) is no longer being detected by the copper-distribution shelf power converter.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	For line drawer A, perform a protection switch from the primary LIC to the secondary LIC. *This causes the primary LIC to become the secondary LIC.*
2	If the alarm clears, replace the LIC from which service was switched. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
3	If the alarm persists, perform a protection switch from the primary LIC to the secondary LIC in line drawer B. *This causes the primary LIC to become the secondary LIC.*
4	If the alarm clears, replace the LIC from which service was switched. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
5	If the alarm persists, replace the copper-distribution shelf power converter that raised this alarm. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
Autoprovisioning mismatch

Probable cause

The circuit pack, card, or module does not belong in the slot in which it has been inserted.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Remove the incorrect circuit pack, card, or module and replace it with the correct unit. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
Both planes non-operational

Probable cause

This alarm is raised when both access interface cards (AIC), transport interface cards (TIC), or OC-3/OC-12 cards have failed, or they are out of service, or a combination of both conditions.

Impact

This is a critical, service-affecting (C, SA) alarm.

Action

Step	Action

Note: Ensure that all AIC, TIC and OC-3/OC12 equipment alarm points are enabled as described in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B. This will prevent potential alarm conditions from being masked.

1 From any network element screen, display the list of active alarms:

alarms↵

A list of active alarms appears on screen.

2 Look for an alarm raised against the TIC, AIC or OC-3/OC-12:

If a TIC, AIC or OC-3/OC-12 alarm	Then
is raised	look up the alarm in this document and proceed accordingly
is not raised	go to step 3

3 Check the state of AIC A and B:

Note: Both AIC A and B are active in normal operation. There is no primary or secondary AIC. If AIC A is displayed on the AIC equipment screen, then AIC B is the redundant unit.

eq aic a↵

The AIC equipment screen appears.

If	Then
both AICs are OOS	go to step 4
one AIC is IS and the other AIC is OOS	go to step 5
either AIC state is Trbl	go to step 5

—continued—

EQP CE
Both planes non-operational (continued)

Step	Action
4	Change the state of AIC A to in-service: **chgstate is**↵ *The state changes to in-service.*
5	Check the state of the primary and the secondary TIC as follows: ***Note:*** Either TIC (A or B) can act as the primary TIC. The primary or secondary TIC status is changed by a switch of activity. If TIC A is displayed on the TIC equipment screen, then TIC B is the redundant unit. The redundant unit can be either the primary or secondary TIC. **a.** Display the TIC equipment screen and select TIC A: **eq tic a**↵ *The TIC equipment screen appears as shown.* **b.** Query the status of the primary and secondary TIC: **query**↵ *The state and status information for TIC A and B appears in the work area of the TIC equipment screen.*

If	Then
both TICs are OOS	a. Determine if TIC A is the primary TIC. If it is, go to step 6. b. If TIC A is the secondary TIC, select TIC B: **select b**↵ c. Go to step 6.
the primary TIC is IS and the secondary TIC is OOS	go to step 7
either TIC state is Trbl	go to step 7

6	Change the state of the primary TIC to in-service: **chgstate is**↵ *The state changes to in-service.*

—continued—

EQP CE
Both planes non-operational (continued)

Step	Action

7 Check the state of the active and standby OC-3/OC-12 units as follows:

a. Access the OC-3/OC-12 equipment screen and select unit g1.

eq <optical type> g1↵

where

<optical type> is the type of optical equipment: **oc3** or **oc12**

b. Query the state and status of unit G1 and G2:

query↵

The OC-3 or OC-12 equipment screen appears showing the state and status for the active and standby units.

If	Then
both OC-3/OC-12 units are OOS	go to step 8
the active unit is IS and standby unit is OOS	go to step 10
either OC-3/OC-12 unit is Trbl	go to step 10

8 Determine if group G1 is the active OC-3/OC-12 unit.

If group G1 is the	Then
active unit	go to step 9.
standby unit	a. Select the active OC-3/OC-12 unit: **select g2**↵ b. Go to step 9.

9 Change the state of the active OC-3/OC-12 unit to in-service:

chgstate is↵

The state changes to in-service.

If this alarm	Then
clears	end the procedure
persists	go to step 10

10 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
CNet link fail

Probable cause

The processor (Proc) can not communicate through the CNet with any other Proc or with the OPC for one of the following reasons:

- one of the processors in a network element is defective
- the CNet cable or termination plug is defective or disconnected
- one of the processor circuit packs at an RFT is removed

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

If one of the processor circuit packs at an RFT is removed, replace the processor. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

For troubleshooting information refer to “CNet performance degraded” on page 3-52.

—end—

Eqp CE
CNet performance degraded

Probable cause

The system has detected a problem with the CNet cabling or connections. In some cases, this alarm can be caused by a Processor or OPC hardware fault.

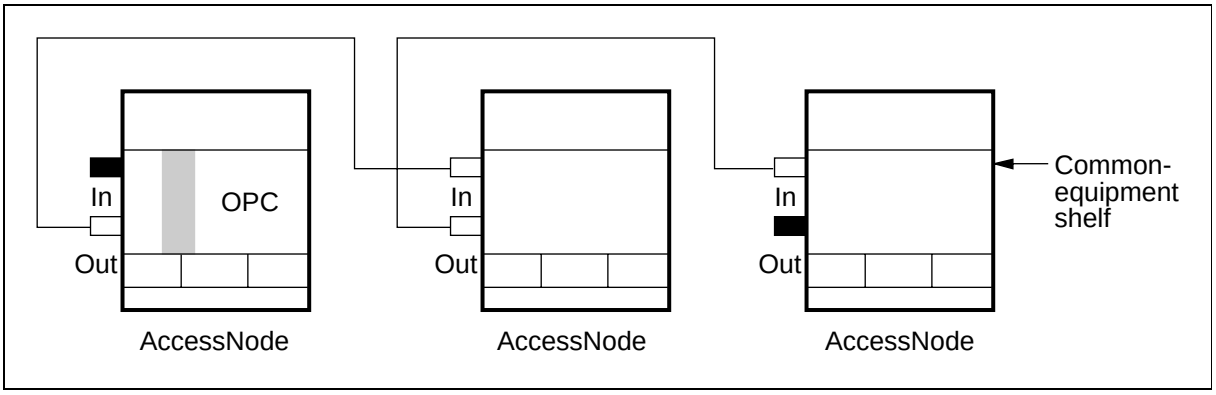
Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	Verify the control network cabling at each connection point on each shelf. The following figure shows a block diagram of a typical CNet connection between three common-equipment shelves. The output of one shelf connects to the input of the next shelf. Unused CNet connectors must be terminated with an NT7E5072 termination plug. Defective cabling or termination plugs have been known to cause these alarms (link or performance degraded). If the alarm cannot be cleared after checking cable installation, try another cable/termination plug or verify the pin-outs listed in *Bay in Central Office Installation Manual for ABM,* 323-3001-201.

PC-10150



If the CNET cabling and connectors are properly installed, check for equipment alarms raised against the Processor or OPC at each location on the LAN. Solve these alarms as instructed in this document.

—end—

Eqp CE
Critical test alarm

Probable cause

This alarm is raised by the FWALTSCI tool, which is used to test the generation of a critical alarm.

Impact

This is a critical, not service-affecting (C, nsa) alarm, for testing purposes only.

Action

Step	Action
1	Access the FiberWorld Alarm Test CI (fwaltsci) tool by entering the following command from the command interpreter level of the user interface, or from any FWPUI screen: **fwaltsci** ↵ *The following prompt appears: "fwaltsci".*
2	Clear the test alarm: **clear critical** ↵ *The critical test alarm clears.*
3	Quit out of the fwaltsci tool: **quit** ↵
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
Database not restored. Type Q APPROVE at NE

Probable cause

The network element recovered from a (reload) restart without a valid backup database being restored from RAM or from the OPC.

The DATABASE NOT RESTORED alarm represents a serious condition and needs to be addressed promptly, as there is a potential for service to be affected. Low-speed (DS1 and DS3) protection is *not available* while this condition exists. When this condition exists, an up-to-date database for the node may be restored from tape to the OPC and then the node rebooted. Alternatively, all service-affecting parameters may be re-edited and the APPROVE command used.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

The following procedure clears this alarm in either of two ways: one method, which is the preferred method, is performed from the OPC when a backup tape is available; the other method, which requires you to verify each provisionable parameter on the NEUI, should be used only if a tape backup is not available. After verifying each parameter, the APPROVE command is used.

The APPROVE command is used to indicate that all equipment and facility parameters have been verified as correct, and are approved for use on the hardware.

If the APPROVE command is executed before all parameters are corrected, SERVICE WILL BE AFFECTED. Warning messages indicating TRAFFIC WILL/MAY BE LOST can be ignored when editing facility parameters during this mode of operation. Hardware continues to carry traffic while facilities are being edited.

—continued—

Eqp CE
Database not restored. Type Q APPROVE at NE (continued)

Step	Action
1	Determine if you have a recent OPC tape backup available.

If a recent OPC tape backup	Then
is available	do step 2
is not available	do step 3

2	Restore OPC data from tape. See *Data Administration Procedures*, 323-3001-304, in *Operations, Administration, and Provisioning*, Volume 4A. End the procedure here.
3	Using office records, verify the settings of all editable parameters. For reference, see the 300-series of documentation in *Operations, Administration and Provisioning*, Volume 4. When all parameters have been restored, enter the following from the network element status screen to approve all database settings and restart the NE: **approve** ↵ **yes** ↵ *The approve command initiates a restart of the processor.*
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
Entry to SONET clock freerun

Probable cause

The shelf has reverted to its SONET clock despite being provisioned for ESI timing.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Check for one or more ESI subunit failures. Clearing these failures will clear this alarm.

Step	Action

1 From the network element status screen, display the ESI equipment screen:

eq esi <circuit group>↵

where

<circuit group> is **g1** or **g2**

The ESI equipment screen appears.

If the ESI card is	Then
IS	Repeat step 1 for the second ESI card if applicable. Go to step 2.
OOS	Change the state of the ESI card to IS: **chgstate is**↵ Repeat step 1 for the second ESI card if applicable. Go to step 2.

2 Determine if the alarm clears.

If the alarm	Then
clears	end the procedure
persists	go to step 3

—continued—

Eqp CE
Entry to SONET clock freerun (continued)

Step	Action
3	Access the ESI facility screen: **fa esi <timing reference>**↵ where <timing reference> is **bitsa** or **bitsb** **query all**↵ *The ESI facility appears.*
4	Check that the ESI facility unit states are in service (IS), and the parameters in effect for the facility are correct.

If the ESI	Then
facilities are IS and the parameters are correct	go to step 6
facilities are not IS or the parameters are incorrect	Return the ESI facilities to service or correct the ESI interface parameters as required (see *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B, for details on provisioning ESI parameters). Go to step 5.

5 Determine if the alarm clears.

If the alarm	Then
clears	end the procedure
persists	go to step 6

6 Firmly reseat the ESI carrier (for details see the ESI carrier module replacement procedure in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If the alarm	Then
clears	end the procedure
persists	go to step 7

—continued—

Eqp CE
Entry to SONET clock freerun (continued)

Step	Action

7 Firmly reseat each ESI card in the ESI carrier (for details see the ESI module replacement procedure in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If the alarm	Then
clears	end the procedure
persists	go to step 8

8 Replace one or both of the ESI cards (if required) as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If the alarm	Then
clears	end the procedure
persists	go to step 9

9 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
Exerciser fail

Probable cause

The protection exerciser is not able to complete successfully. The cause of this alarm is recorded exerciser log.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Determine why the exerciser failed by reading the Eqp 608 log. At the prompt type: **logutil** ↵ **open eqp** ↵
2	Clear the problem indicated in the log. The log could indicate the following results, which would raise the Exerciser fail alarm. • failed: diagnostic failed or software errors • failed: facility out of service • aborted: due to circuit pack removal • aborted: exerciser run prematurely terminated by a higher priority system activity
3	Run the exerciser again to clear the alarm.

—end—

Eqp CE
Loss of data synchronization

Probable cause

The data synchronization enable/disable option has been set to "off." Software failures can also cause this alarm.

Note: A craftsperson should not perform a switch of activity (SWACT) when this alarm is generated.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	Set the data synchronization enable/disable option to "on." See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B.

If the alarm	Then
clears	You have completed the procedure.
persists	A software failure might be causing the alarm. Contact Nortel Networks for a resolution.

—end—

Eqp CE
Major test alarm

Probable cause

This alarm is raised by the FWALTSCI tool, which is used to test the generation of a major alarm.

Impact

This is a major, not service-affecting (M, nsa) alarm, for testing purposes only.

Action

Step	Action
1	Access the FiberWorld Alarm Test CI (fwaltsci) tool by entering the following command from the command interpreter level of the user interface, or from any FWPUI screen: **fwaltsci** ↵ *The following prompt appears: "fwaltsci".*
2	Clear the test alarm: **clear major** ↵ *The major test alarm clears.*
3	Quit out of the fwaltsci tool: **quit** ↵
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
Minor test alarm

Probable cause

This alarm is raised by the FWALTSCI tool, which is used to test the generation of a minor alarm.

This alarm is raised by the FWALTSCI tool, which is found at the command interpreter level (CI) of the network element user interface.

Impact

This is a minor, not service-affecting (m, nsa) alarm, for testing purposes only.

Action

Step	Action
1	Access the FiberWorld Alarm Test CI (fwaltsci) tool by entering the following command from the command interpreter level of the user interface, or from any FWPUI screen: **fwaltsci** ↵ *The following prompt appears: "fwaltsci".*
2	Clear the test alarm: **clear minor** ↵ *The minor test alarm clears.*
3	Quit out of the fwaltsci tool: **quit** ↵
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
Plane A non-operational

Probable cause

The access interface card (AIC) or transport interface card (TIC) in group A has failed, or is out of service.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	From any network element screen, display the list of active alarms: **alarms**↵ *A list of active alarms appears on screen.*
2	Look for an alarm raised against a TIC or AIC.

If a TIC or AIC alarm	Then
is raised	look up the alarm in this document and proceed accordingly
is not raised	go to step 3

Step	Action
3	Check the state of the AIC on plane A: **eq aic a**↵ *The AIC equipment screen appears.*

If the state of AIC-A is	Then
OOS	go to step 4
IS	go to step 5

—continued—

Eqp CE
Plane A non-operational (continued)

Step	Action
4	Change the state of the AIC to in-service: **chgstate is**↵ *The state changes to in-service.*
5	Check the state of the TIC on plane A: **eq tic a**↵ *The TIC equipment screen appears.*

If the state of TIC-A is	Then
OOS	go to step 6
IS	go to step 7

6	Change the state of the TIC to in-service: **chgstate is**↵ *The state changes to in-service.* If the alarm clears, end the procedure here. If the alarm persists, go to step 7.
7	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
Plane B non-operational

Probable cause

The access interface card (AIC) or transport interface card (TIC) in group B has failed, or is out of service.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	From any network element screen, display the list of active alarms: **alarms**↵ *A list of active alarms appears on screen.*
2	Look for an alarm raised against a TIC or AIC.

If a TIC or AIC alarm	Then
is raised	look up the alarm in this document and proceed accordingly
is not raised	go to step 3

Step	Action
3	Check the state of the AIC on plane B: **eq aic b**↵ *The AIC equipment screen appears.*

If the state of AIC-B is	Then
OOS	go to step 4
IS	go to step 5

—continued—

Eqp CE
Plane B non-operational (continued)

Step	Action
4	Change the state of the AIC to in-service: **chgstate is**↵ *The state changes to in-service.*
5	Check the state of the TIC on plane B: **eq tic b**↵ *The TIC equipment screen appears.*

If the state of TIC-B is	Then
OOS	go to step 6
IS	go to step 7

6	Change the state of the TIC to in-service: **chgstate is**↵ *The state changes to in-service.* If this alarm clears, end the procedure here. If the alarm persists, go to step 7.
7	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
Ring reconfiguration in progress

Probable cause

A craftsperson is reconfiguring the ring.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

No action is required.

—end—

Eqp CE
Shelf assembly fail

Probable cause

This alarm can be raised for one of the following reasons:

- There is a problem with one of the side interconnect cards on the common-equipment shelf.
- One of the I/O cards in the I/O portion of the common-equipment shelf is improperly seated.
- A problem exists with one of the CBIC-based cards on CBUS plane B.

Impact

This is a critical, service-affecting (C, SA) alarm.

Action

On ABM and TBM shelves, check for proper seating of the side interconnect left card located in the far left slot of the common-equipment shelf.

On ABM shelves with associated copper-distribution shelves, check for proper seating of the side interconnect right card located in the far right slot of the shelf.

Check for an improperly seated I/O card in the I/O portion of the common-equipment shelf.

If the above cards are properly seated in their respective slots, and this alarm does not clear, contact your Nortel Networks service representative and report a possible problem with CBIC-based cards on CBUS plane B.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
Shelf ID bus fail

Probable cause

This alarm can be raised for one of the following reasons:

- There is a problem with the NT4K2030 shelf identification card, which is installed on the shelf backplane.
- One of the I/O cards in the I/O portion of the common-equipment shelf is improperly seated.
- A problem exists with one of the CBIC-based cards on CBUS plane B.

Impact

This is a major, not service-affecting (M, nsa) alarm.

Action

Check for an improperly seated I/O card in the I/O portion of the common-equipment shelf.

If the I/O cards appear to be properly seated, contact your Nortel Networks service representative and report a possible problem with the NT4K2030 shelf identification card, or one of the CBIC-based cards on CBUS plane B.

> ***Note:*** If the NT4K2030 ID card is replaced, and the shelf ID programmed into the replacement card is different from the original card, an SDA352 OPC log may be generated. The SDA352 log indicates a commissioning error, because of a mismatch between the serial number of the network element, and the serial number programmed into the new ID card.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
Software trap

Probable cause

A software trap has occurred in the software load.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Contact Nortel Networks and report the alarm.

—end—

Eqp CE
SONET overhead data/clock loss

Probable cause

A clock loss has been detected on the SONET overhead bus, due to an incorrect fiber connection error, a faulty processor card, or a faulty OC-3/OC-12 optical interface.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

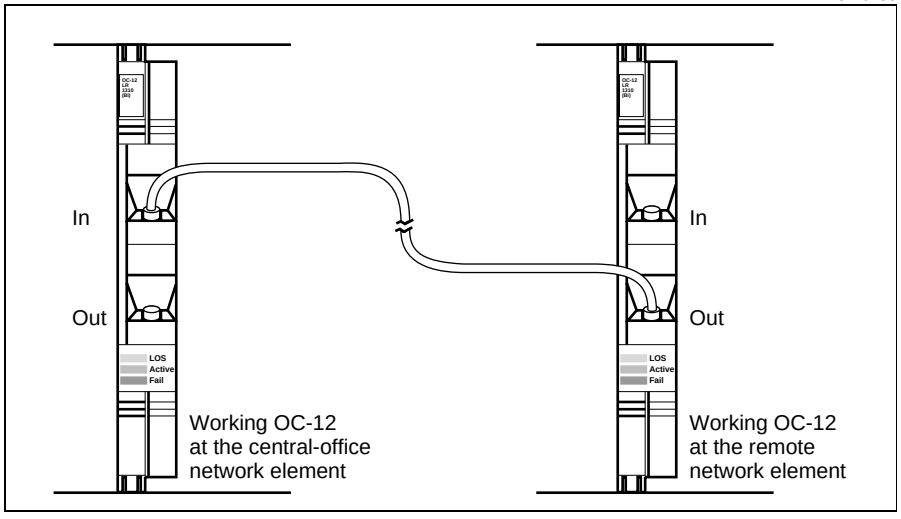
Step	Action

1 Verify all origination and termination points for the fiber-optic cables connected to the optical circuit packs. Fibers from the G1 (working) optics at the FCOT must connect to the G1 (working) optics at the RFT. The proper connection is from receiver (Rx) to transmitter (Tx).

If fiber-optic cables are	Then
not properly connected	go to step 2
properly connected	go to step 3

2 Connect fibers from the G1 (working) optics at the FCOT to the G1 (working) optics at the RFT. The following figure shows how the OC-12 Rx at one end connects to the Tx at the other OC-12 (same for OC-3). Only one connection is shown for clarity. There is a corresponding Tx to Rx connection.

PC-10783



—continued—

Eqp CE
SONET overhead data/clock loss (continued)

Step	Action

If this alarm	Then
clears	end the procedure
persists	go to step 3

3 One at a time, replace the active (working) optical interfaces, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	The original card was faulty. End the procedure.
persists	go to step 4.

4 Replace the redundant (standby) processor, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	The original card was faulty. End the procedure.
persists	go to step 5

5 Replace the primary (active) processor, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	The original card was faulty. End the procedure.
persists	if you cannot successfully complete this procedure, contact your next level of support

—end—

Eqp CE
Timing generation primary reference fail
Timing generation secondary reference fail

Probable cause

The external synchronization interface (ESI) card cannot synchronize to the primary or secondary timing reference. This can be caused by a reference frequency outside the Stratum 3 range, or excessive transients on the primary reference signal.

Note: The ESI card automatically detects and switches away from timing reference sources that fail or significantly deviate from acceptable stratum levels (for example, Stratum 3 range). The timing reference source is derived from the central office's building integrated timing source (BITS), either BITSCC or BITSDS1.

Upon failure of the active timing reference, both ESI circuit packs switch to their secondary timing source and one alarm is raised, depending on which reference failed.

If both timing references fail, both alarms are raised (with the "Timing generation primary reference fail" alarm classified as major) and ESI enters the Holdover or ESI Freerun mode, depending on the current state of the Current Filter Mode. The following table summarizes the Current Filter Mode states before and after failure of both timing references:

Current filter mode	
Before fault	**After fault**
Freerun	Freerun
Acquire	Freerun
Fast	Holdover
Normal	Holdover
Holdover	Holdover
Note: Freerun means ESI freerun, not SONET freerun.	

—continued—

Eqp CE
Timing generation primary reference fail
Timing generation secondary reference fail (continued)

Note: Under timing deviation conditions, the ESI Current Filter Mode usually is in the Acquire mode prior to the fault being declared. As a result, the post-fault condition for this case is usually ESI Freerun.

Several other ESI related alarms, including Fac ESI Loss of frame, Fac ESI Loss of signal, Fac ESI Rx AIS, might be present.

Impact

If one timing generation reference fail alarm is raised (either the primary or secondary), this is a minor, not service-affecting (m, nsa) alarm.

If both alarms are raised simultaneously, the individual alarm impact is as follows:

- Timing generation primary reference fail, major, not service-affecting (M, nsa) alarm.
- Timing generation secondary reference fail, minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Check the ESI cable and the presence and accuracy of BITS timing sources. ***Note:*** Ensure that the ESI cable is properly connected at the external timing reference (BITS) and at the appropriate jack on the side interconnect left card of the common-equipment shelf. For details see the procedure for setting up external synchronization in *Commissioning and Testing,* Volume 3.
2	Ensure that the provisioned ESI parameters are correct for the timing source. (See the procedure for provisioning ESI parameters in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B.)
3	Ensure that any external reference inputs being used as timing sources are in service (IS).

—continued—

Eqp CE
Timing generation primary reference fail
Timing generation secondary reference fail (continued)

Step	Action
4	Access the protection screen by entering: **protectn** ↵ *The protection screen appears.*
5	Access the ESI reference protection screen by entering: **trefprot esi** ↵

CAUTION
Temporary loss of synchronization
Performing repeated reference switches without allowing time for the system to lock to the active reference can cause a temporary loss of synchronization with the timing reference source. Wait 30 seconds before repeating a manual switch on a timing reference facility.

6 Perform a manual switch of activity to the restored reference by entering:

manual op <timing reference> ↵

yes ↵

where

<timing reference> is the timing reference (**pri** or **sec**) that is currently active

The screen displays an asterisk (*) under the heading `Manual`.

Note: A manual switch of an ESI timing reference is indicated by a transition from normal (.) to active (*) and back to normal (.).

—continued—

Eqp CE
Timing generation primary reference fail
Timing generation secondary reference fail (continued)

Step	Action
7	Determine if the alarm clears.

If the alarm	Then
clears and there is no other alarm of this type raised	a. Remove the manual protection switch: **manual re <timing reference>**↵ where <timing reference> is **pri** or **sec** b. End the procedure
clears, but there is a second alarm of this type raised	a. Remove the manual protection switch: **manual re <timing reference>**↵ where <timing reference> is **pri** or **sec** b. Go to step 2 and work through the steps to the end of the procedure to clear the second alarm
persists	If the restored signals remains out of Stratum specification, the same alarms are again raised. The accuracy of the references must be examined further. Go to step 8.

8	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
Traffic upgrade in progress

Probable cause

This alarm indicates that a traffic upgrade is in progress.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

None.

—end—

Eqp CE
Warning test alarm

Probable cause

This alarm is raised by the FWALTSCI tool, which is used to test the generation of a warning alarm.

Impact

This is a minor, not service-affecting (m, nsa) alarm, for testing purposes only.

Action

Step	Action
1	Access the FiberWorld Alarm Test CI (fwaltsci) tool by entering the following command from the command interpreter level of the user interface, or from any FWPUI screen: **fwaltsci** ↵ *The following prompt appears: "fwaltsci".*
2	Clear the test alarm: **clear warning** ↵ *The warning test alarm clears.*
3	Quit the fwaltsci tool: **quit** ↵
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp CE
User port 1 intrusion attempt
User port 2 intrusion attempt
User port 3 intrusion attempt
User port 4 intrusion attempt

Probable cause

More than the allowable number of unsuccessful log-in attempts have been made from the equipment connected to the user interface port identified in the alarm. A log-in attempt is unsuccessful if either the user identifier or password entered is invalid.

The allowable number of unsuccessful log-in attempts ranges from 2 to 9, as provisioned through the Centralized User Administration tool (see *System Administration Procedures*, 323-3001-302, in *Operations Administration and Provisioning*, Volume 4A).

This alarm is raised when the user interface port has been locked out and clears when the port is unlocked. The port is unlocked automatically after a set period of time, called the alert duration period, which is also provisionable through the Centralized User Administration tool.

Impact

Minor alarm, non-service affecting.

Enabled by default (unprovisionable).

The user interface port is locked out when the maximum number of log-in attempts for that port has been exceeded. No user can log in to the network element through that port until the provisioned alert duration period has expired. The alert duration period can be up to 3 minutes.

Action

No user action is required to clear the alarm. It clears automatically on the expiry of the alert duration period. However, the system administrator might wish to investigate to ensure that there has not been an unauthorized attempt to breach network security.

—end—

Eqp DS1
Circuit pack fail

Probable cause

The DS1/VT mapper circuit pack failed.

Impact

If this is a critical, service-affecting (C, SA) alarm, traffic has not switched to a backup circuit pack, and DS1 traffic is lost.

If this is a minor, not service-affecting (m, nsa) alarm, DS1 traffic has switched to a backup circuit pack, or there was no traffic associated with the circuit pack when it failed.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Circuit pack mismatch

Probable cause

The alarm can be caused by any of the following conditions:

- the circuit pack in the slot designated for the DS1 does not match the provisioned circuit pack.
- the DS1/VT protection mapper is an NT7E04BA circuit pack and one or more of the working DS1/VT mappers is an NT7E04CA circuit pack.

  Note 1: If a DS1 is carrying TR-08 traffic, it must be provisioned on an NT7E04CA DS1/VT mapper. The protection DS1/VT mapper must also be an NT7E04CA circuit pack if any of the working mappers on a common-equipment shelf are carrying TR-08 traffic. Otherwise, TR-08 traffic will be lost if a protection switch occurs.

  Note 2: If a DS1 is provisioned to carry Byte Synchronous traffic, this alarm is raised if an NT7E04AA mapper is inserted into that slot.

Impact

If this is a critical, service-affecting (C, SA) alarm, traffic could not be switched to a backup circuit pack, and DS1 traffic is lost.

If this is a minor, not service-affecting (m, nsa) alarm, DS1 traffic has switched to a backup circuit pack, or there was no traffic associated with the circuit pack.

Action

Determine if any of the working DS1/VT mappers are NT7E04CA circuit packs. For slot information see “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15. If there are any NT7E04CA working mappers on the shelf, ensure that the protection mapper is also an NT7E04CA circuit pack. For details on replacing a DS1/VT mapper see *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If the circuit pack in the slot designated for the DS1 does not match the provisioned circuit pack, replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code. For details see *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

—continued—

Eqp DS1
Circuit pack mismatch (continued)

If Byte Synchronous traffic is a requirement for any facility on that slot, check the version of the DS1/VT mapper installed in the shelf. To support Byte Synchronous traffic the working DS1/VT mapper must have a product engineering code of NT7E04BA or higher. If Byte Synchronous is not a requirement, change the DS1 parameters for the facility. See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Circuit pack missing

Probable cause

A slot provisioned for a DS1/VT mapper does not contain a DS1/VT mapper circuit pack.

Impact

If this is a critical, service-affecting (C, SA) alarm, traffic could not be switched to a backup circuit pack, and DS1 traffic is lost.

If this is a minor, not service-affecting (m, nsa) alarm, DS1 traffic has switched to a backup circuit pack, or there was no traffic associated with the circuit pack.

Action

If the circuit pack is present in the slot, ensure that it is properly seated.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If this alarm persists after waiting 3 or 4 minutes, or if the DS1 equipment screen shows the replaced card as UEQ, replace the active processor circuit pack, as described in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Facility provisioning mismatch

Probable cause

Either the working or protection DS1/VT mapper does not support the service that is provisioned on one of the DS1 facilities associated with the mapper. The unsupported service is either

- TR-08 or
- a provisioning combination of B8ZS line coding and AZC alarm encoding
- Byte Synchronous traffic when an NT7E04AA mapper is inserted into that slot

Impact

This is a major, service-affecting (M, SA) alarm.

Action

If TR-08, or a combination of B8ZS line coding and AZC alarm encoding, or Byte Synchronous is a requirement, check the version of the DS1/VT mapper installed in the shelf. To support TR-08, or a combination of B8ZS line coding and AZC alarm encoding, the DS1/VT mapper must have a product engineering code of NT7E04CA or higher. Also, to support Byte Synchronous, the DS1/VT mapper must have a product engineering code of NT7E04BA or higher. If an incorrect working or protection DS1/VT mapper is installed, replace it with the correct circuit pack, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If TR-08, or a combination of B8ZS line coding and AZC alarm encoding, or Byte Synchronous is not a requirement, change the DS1 parameters for the facility. See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Forced switch request

Probable cause

A forced switch was requested, for one of the DS1/VT mapper circuit packs.

Impact

This is a minor, non-service-affecting (m, nsa) alarm. The alarm will clear when the forced switch is released. If the forced switch request is not cleared, the protection unit will not be available for use by the other working DS1/VT Mapper circuit packs in the event of a problem.

Note: An EQP606 log is generated each time protection activity occurs.

Action

No action is required. If you want to release the forced switch request, follow this procedure.

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr**↵ *The protection switching screen appears.*
2	Display the detailed protection screen: **dtlprot ds1**↵ *The detailed protection screen appears.*
3	Release the forced switch: **forced re < group >**↵ **y**↵ where < group > number of the circuit pack group: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15 for values. *The screen displays a period (.) in the* `Forced` *column for the corresponding group.*
4	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Eqp DS1
Input card fail -DoNotRemove

Probable cause

The ID PROM, on a DS1 input card, is failed or is incorrectly programmed, but the card is still functional.

Impact

If this alarm is raised against an input card that has one or more facilities that are in service, this alarm is major, not service-affecting (M, nsa) alarm.

If this alarm is raised against an input card that has no in-service facilities, this alarm is minor, not service-affecting (m, nsa).

Action

No immediate action is required. Schedule a card replacement of the DS1 input card during a low traffic period if the card is carrying traffic. Replace the card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Input card mismatch

Probable cause

The incorrect card is in the slot designated for a DS1 input card.

> ***Note:*** For information on I/O card slot associations, see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15.

Impact

If this is a critical, service-affecting (C, SA) alarm, traffic is lost on the 14 DS1 lines associated with this card.

If this is a minor, not service-affecting (m, nsa) alarm, there is no traffic associated with this card.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Input card missing

Probable cause

A DS1 input card is missing.

> ***Note:*** For information on I/O card slot associations, see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15.

Impact

If this is a critical, service-affecting (C, SA) alarm, traffic is lost on the 14 DS1 lines associated with this card.

If this is a minor, not service-affecting (m, nsa) alarm, there is no traffic associated with this card.

Action

In the empty slot, install a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If a DS1 input card is already in the slot, ensure that it is firmly engaged with the backplane, and the card is screwed down.

If the DS1 input card is properly seated and secured, check for other more severe alarms and proceed with that procedure.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Lockout request

Probable cause

A protection switch lockout is in effect for one of the DS1 circuit pack groups for maintenance purposes.

Impact

This is a minor, non-service-affecting (m, nsa) alarm. If a working DS1 group is locked out, the system can not switch service to the protection unit in the event of a problem. If the DS1 protection group is locked out, protection is not available for any working DS1 group.

Note: An EQP606 log is generated each time protection activity occurs.

Action

No action is required. If you want to release the lockout, follow this procedure.

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr**↵ *The protection switching screen appears.*
2	Display the detailed protection screen: **dtlprot ds1**↵ *The detailed protection screen appears.*
3	Release the lockout: **lockout re < group >**↵ **y**↵ where < group > number of the circuit pack group: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15 for values. *The screen displays a period (.) in the* `Lockout` *column for the corresponding group.*
4	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Eqp DS1
Manual switch request

Probable cause

The manual protection switch command was entered against a DS1 group.

Impact

This is a minor, non-service-affecting (m, nsa) alarm. In the event of a problem with the other DS1 group, the system will override the manual request, and switch it to the protection group.

Note: An EQP606 log is generated each time protection activity occurs.

Action

No action is required. If you want to release the manual switch request, follow this procedure.

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr**↵ *The protection switching screen appears.*
2	Display the detailed protection screen: **dtlprot ds1**↵ *The detailed protection screen appears.*
3	Release the manual switch: **manual re < group >**↵ **y**↵ where < group > number of the circuit pack group: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15 for values. *The screen displays a period (.) in the* `Manual` *column for the corresponding group.*
4	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Eqp DS1
Output card fail - DoNotRemove

Probable cause

The ID PROM, on a DS1 output card, is failed or is incorrectly programmed, but the card is still functional.

Impact

If this alarm is raised against an output card that has one or more facilities that are in service, this alarm is major, not service-affecting (M, nsa) alarm.

If this alarm is raised against an output card that has no in-service facilities, this alarm is minor, not service-affecting (m, nsa).

Action

No immediate action is required. Schedule a card replacement of the DS1 output card during a low traffic period if the card is carrying traffic. Replace the card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Output card mismatch

Probable cause

The incorrect card is in the slot designated for a DS1 output card.

> ***Note:*** For information on I/O card slot associations, see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15.

Impact

If this is a critical, service-affecting (C, SA) alarm, traffic is lost on the 14 DS1 lines associated with this card.

If this is a minor, not service-affecting (m, nsa) alarm, there is no traffic associated with this card.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Output card missing

Probable cause

A DS1 output card is missing.

> ***Note:*** For information on I/O card slot associations, see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15.

Impact

If this is a critical, service-affecting (C, SA) alarm, traffic is lost on the 14 DS1 lines associated with this card.

If this is a minor, not service-affecting (m, nsa) alarm, there is no traffic associated with this card.

Action

In the empty slot, install a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If a DS1 output card is already in the slot, ensure that it is firmly engaged with the backplane, and the card is screwed down.

If the DS1 output card is properly seated and secured, check for other more severe alarms and proceed with that procedure.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Prot bridge in card fail -DoNotRemove

Probable cause

The ID PROM, on a DS1 protection bridge in card, has failed or is incorrectly programmed.

Impact

If this alarm is raised against a protection bridge card that has one or more facilities that are in service, this alarm is major, not service-affecting (M, nsa) alarm.

If this alarm is raised against a protection bridge card that has no in-service facilities, this alarm is minor, not service-affecting (m, nsa).

Action

No immediate action is required. Schedule a card replacement of the DS1 protection bridge card during a low traffic period if the card is carrying traffic. Replace the card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Prot bridge in card mismatch

Probable cause

The incorrect card is in the slot designated for a protection bridge card for the DS1 inputs.

In a TBM shelf the DS1 protection bridge in card is located in slot 42, and in an ABM shelf in slot 34.

Impact

If this is a critical, service-affecting (C, SA) alarm, traffic is lost on one of the DS1 input cards.

> ***Note:*** Note: Only a forced switch from one of the working DS1s can cause the critical severity. Traffic will remain lost until the forced switch is released, or the mismatched card is replaced with the correct card.

If this is a minor, not service-affecting (m, nsa) alarm, traffic is not affected.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Prot bridge in card missing

Probable cause

The protection bridge card is missing for the DS1 inputs.

In a TBM shelf the DS1 protection bridge in card is located in slot 42, and in an ABM shelf in slot 34.

Impact

If this is a critical, service-affecting (C, SA) alarm, traffic is lost on one of the DS1 input cards.

> ***Note:*** Only a forced switch from one of the working DS1s can cause the critical severity. Traffic will remain lost until the forced switch is released, or the missing card is replaced with the correct card.

If this is a minor, not service-affecting (m, nsa) alarm, traffic is not affected.

Action

In the empty slot, install a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Prot bridge out card fail -DoNotRemove

Probable cause

The ID PROM, on a DS1 protection bridge out card, is failed or is incorrectly programmed.

Impact

If this alarm is raised against a protection bridge card that has one or more facilities that are in service, this alarm is major, not service-affecting (M, nsa) alarm.

If this alarm is raised against a protection bridge card that has no in-service facilities, this alarm is minor, not service-affecting (m, nsa).

Action

No immediate action is required. Schedule a card replacement of the DS1 protection bridge card during a low traffic period if the card is carrying traffic. Replace the card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Prot bridge out card mismatch

Probable cause

The incorrect card is in the slot designated for a protection bridge card for the DS1 outputs.

In a TBM shelf the DS1 protection bridge out card is located in slot 44, and in an ABM shelf in slot 36.

Impact

If this is a critical, service-affecting (C, SA) alarm, traffic is lost on one of the DS1 output cards.

If this is a minor, not service-affecting (m, nsa) alarm, traffic is not affected.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Prot bridge out card missing

Probable cause

A DS1 protection bridge out card is missing from its slot (TBM shelf slot 44, or ABM shelf slot 36).

Impact

If this is a critical, service-affecting (C, SA) alarm, there was a protection switch active and DS1 traffic is lost. The duration of the traffic loss depends on the DS1 protection switching conditions at the time the protection bridge out card was removed. Because of the polling method, it takes 4 to 6 seconds for the system to detect a missing protection bridge out card. Traffic is lost during this detection time, but once detected one of the following can occur:

- For a manual protection switch, traffic is switched back to the working DS1 group within 30 milliseconds. This alarm remains critical during the 30-millisecond period, then the severity changes to minor, not service affecting (m, nsa).
- For an automatic fault protection switch, traffic is switched back to the working DS1 group within 30 milliseconds. This alarm remains critical during the 30-millisecond period, then the severity changes to minor, not service affecting (m, nsa). After protection is dropped, the alarm severity for the faulty DS1 group increases to critical.
- For a forced protection switch, service is lost. This alarm remains critical until the protection bridge card is replaced. The system does not attempt to switch back to a working mapper.

  Note: In the case of a forced protection switch, an alarm indication signal (AIS) is sent to the far end where a “VT Rx AIS” alarm is raised. The far-end network element confirms the AIS by returning a “yellow” signal. The yellow signal would typically raise the alarm “VT Rx yellow,” however, the alarm “Prot bridge out card missing” is more severe and masks this alarm from being raised.

If this is a minor, not service-affecting (m, nsa) alarm, no protection switch was active, and DS1 traffic is not affected.

—continued—

Eqp DS1
Prot bridge out card missing (continued)

Action

Install a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If a forced protection switch is active when the protection bridge card is removed, the “VT Rx yellow” alarm, which was previously masked, appears and remains for 30 seconds.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Protection path fail

Probable cause

System diagnostics failed while attempting to bridge traffic from a working DS1 group to the DS1 protection group. This indicates that a hardware failure exists on the DS1 protection path.

Note: The presence of a low DS1 signal level on the DS1 facility has been known to cause this alarm. The protection unit is unable to detect the signal when traffic is bridged to it.

Impact

While this alarm is in effect, service cannot be switched to the protection DS1 group in the event of a problem with the working DS1/VT mappers. If a DS1 working circuit pack needs to be protected and a failure exists on the protection path, this alarm is raised as a major alarm since traffic is lost. If no protection is required, the unprotected severity is minor.

In a protected configuration, this is a major, service-affecting (M, SA) alarm.

In an unprotected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	From the DS1 protection equipment screen, check the state of the DS1 protection group and check if there are unequipped cards. **eq ds1 p**↵ *The DS1 protection equipment screen appears.*

If the state field indicates	Then
IS - Trbl or Ueq	go to step 2
OOS	go to step 3
IS - Normal	go to step 5

—continued—

Eqp DS1
Protection path fail (continued)

Step	Action
2	Replace defective or missing (Ueq) cards as indicated in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C. Go to step 4. ***Note:*** On the DS1 equipment screen, the list of cards in the protection group should include one DS1/VT mapper (NT7E04) and two DS1 protection bridge cards (NT4K31).
3	Change the operating state to IS (in service): **chgstate is**↵ *The operating state of the protection group changes to IS.*
4	At the shelf equipment screen, run the DS1 protection exerciser: **eq sh** ↵ **exercise** ↵ If the alarm clears, the procedure is finished. Otherwise, go to step 5.
5	At the MIC equipment screen, verify the state of the maintenance interface circuit pack (MIC): **eq mic**↵ *The MIC equipment screen appears.*

If the MIC state is	Then
OOS	go to step 7
anything other than IS-Normal	go to step 6
IS-Normal	go to step 9

6	Replace the MIC as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C. Go to step 8.
7	Change the operating state of the MIC to IS (in service): **chgstate is** ↵
8	At the shelf equipment screen, run the DS1 protection exerciser: **eq sh** ↵ **exercise** ↵ If the alarm clears, the procedure is finished. Otherwise, go to step 9.

—continued—

Eqp DS1
Protection path fail (continued)

Step	Action
9	Replace the protection DS1/VT mapper, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C. ***Note:*** Parity errors associated with the protection DS1/VT mapper will confirm a fault on this card. Use the **ListAlms** command to obtain a list of alarms.
10	At the shelf equipment screen, run the DS1 protection exerciser: **eq sh** ↵ **exercise** ↵ If the alarm clears, the procedure is finished. Otherwise, go to step 11.
11	Determine which DS1 ports caused the alarm. Type the following at the NE UI prompt: **logutil** ↵ **open flt** ↵ **back** ↵ Type **back**↵ until the Protection path fail log appears. ***Note:*** The FLT700 log that describes this alarm also indicates in its text which DS1 ports caused the failure. It is possible that the ports have a low DS1 signal level that caused the failure. Nortel Networks recommends that you check the signal level of these DS1 ports to determine if this is the cause.
12	Measure the signal level of the affected DS1 ports. If the signal level appears to be significantly lower than the normal DS1 signal level, the low signal level is probably causing the alarm.
13	Access the OC-3/OC-12 protection screen and verify the state of the active OC-3/OC-12 optical interface card in the Rx direction: ***Note:*** Examine the state of the optical circuit pack that has its Rx traffic set to on. **pr;dtlprot <service type>** where <service type> is **oc3** or **oc12** **If the state is** / **Then** IS / go to step 15 other than IS / go to step 14
14	Replace the faulty OC-3/OC-12 optical interface that you identified in step 13, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

—continued—

Eqp DS1
Protection path fail (continued)

Step	Action
15	At the shelf equipment screen, run the DS1 protection exerciser: **eq sh** ↵ **exercise** ↵ If the alarm clears, this procedure is finished. Otherwise, go to step 16.
16	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Protection switch complete

Probable cause

A switch from a working circuit pack to the protection circuit pack was successfully completed.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Note: An EQP606 log is generated each time protection activity occurs.

Action

If the protection switch was a result of a manual or forced switch request for maintenance purposes, no action is required. If the system automatically switched service to the DS1 protection group, check for a DS1 service-affecting alarm, and clear it as outlined in this document.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Protection switch fail

Probable cause

A switch from a working circuit pack to the protection circuit pack was unsuccessful.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Check that there are no lockouts in effect: **eq ds1 all;dtlprot**↵ *The DS1 protection screen appears.*
2	Is there an asterisk (*) in the Lockout column?

If	Then
no	go to step 3
yes	go to step 5

Step	Action
3	Is the operating state IS Normal?

If	Then
no	go to step 4
yes	go to step 7

—continued—

Eqp DS1
Protection switch fail (continued)

Step	Action

4 Display the alarm screen and check for other more severe DS1 protection equipment alarms or MIC equipment alarms.

alarms↵

If	Then
another more severe DS1 equipment alarm appears	look up the alarm in this chapter and proceed accordingly
a MIC equipment alarm appears	look up the alarm in this chapter and proceed accordingly
no other more severe alarms appear	go to step 7

5 Release the lockout:

lockout re < group >↵
y↵

where

< group >	number of the circuit pack group: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15 for values.

The screen displays a period (.) in the `Lockout` *column for the corresponding group.*

6 Retry the protection switch which originally caused this alarm.

If the protection switch	Then
succeeds	end the procedure
fails	go to step 3

—continued—

Eqp DS1
Protection switch fail (continued)

Step	Action

7 Verify the state of the maintenance interface card (MIC):

eq mic↵

If the MIC state is	Then
in service (IS)	go to step 12
out of service (OOS)	go to step 8

8 Perform an out-of-service diagnostic test on the MIC.

Note: Refer to the procedure “Performing a manual diagnostic test” on page 8-10, then return to this point in the procedure.

If the test	Then
passes	go to step 9
fails	go to step 11

9 Change the state of the MIC to in-service:

chgstate is↵

The MIC state changes to in-service (IS).

If the alarm	Then
clears	go to step 10
persists	go to step 11

10 Retry the protection switch which originally caused this alarm.

If the protection switch	Then
succeeds	end the procedure
fails	go to step 11

—continued—

Eqp DS1
Protection switch fail (continued)

Step	Action
11	Replace the MIC, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If the alarm	Then
clears	end the procedure
persists	a. The MIC that was replaced was not faulty. Re-insert the MIC. b. Ensure that the DS1 protection bridge cards are properly seated in their slots. c. Retry the protection switch. If the protection switch succeeds, end the procedure. If it fails, then go to step 12.

12	Replace the protection DS1/VT Mapper, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
13	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
Protection version mismatch

Probable cause

This alarm is raised against the NT7E04CA DS1 mapper to indicate there is a mismatch between the protection mapper version and the mapper version required by the working facility.

The NT7E04CA DS1 mapper is required if the following is provisioned:

- TR08 frame format
- the combination of B8ZS and AZC

Impact

In an unprotected configuration this is a critical, service-affecting (C, SA) alarm.

In a protected configuration this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the NT7E04CA DS1 mapper used for protection, as described in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS1
STS1 intercard fail

Probable cause

A parity error is detected at the backplane between a DS1 mapper and a transport circuit pack (OC -3/OC-12 or Lpbk circuit pack). The cause of the problem might be at the signal source, signal destination or on the signal path. This could be due to a hardware fault that exists on the DS1 mapper, the transport circuit pack, or the backplane.

Impact

This is a critical, service-affecting (C, SA) alarm if the system is in an unprotected configuration and a parity error is detected between an active transport circuit pack and a DS1 mapper.

This is a minor, not service-affecting (m, nsa) alarm if the system is in a protected configuration or a parity error is detected between an inactive transport circuit pack and a DS1 mapper.

Action

Step	Action
1	Display the detailed alarm information for this alarm. See the procedure for displaying a detailed alarm report in *Network Surveillance Procedures*, 323-3001-510, in Maintenance, Volume 5C. The signal source and signal destination are indicated by the primary slot and secondary slot number on the detailed alarm screen. *A screen is displayed*
2	Replace the circuit pack that occupies the primary slot number. See the appropriate procedure in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
3	If the problem persists, replace the circuit pack that occupies the secondary slot number. See the appropriate procedure in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C. ***Note:*** If the alarm clears, the circuit pack replaced is the source of the problem. All other circuit packs replaced before this step are functioning properly and need not be returned to Nortel Networks for repair.
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
BNC I/O card 1 fail -DoNotRemove, BNC I/O card 2 fail -DoNotRemove, BNC I/O card 3 fail -DoNotRemove

Probable cause

The ID PROM, on a BNC I/O card, is failed or is incorrectly programmed, but the card is still functional.

Impact

If this alarm is raised against a BNC I/O card that has a DS3 facility that is in service, this alarm is major, not service-affecting (M, nsa) alarm.

If this alarm is raised against a BNC I/O card that has a DS3 facility that is not in service, this alarm is minor, not service-affecting (m, nsa).

Action

No immediate action is required. Schedule a card replacement of the BNC I/O card during a low traffic period if the card is carrying traffic. Replace the card as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
BNC I/O card 1 mismatch,
BNC I/O card 2 mismatch,
BNC I/O card 3 mismatch

Probable cause

The first, second, or third DS3 I/O card inserted into the shelf I/O slot does not match the provisioned circuit pack type.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Replace the card in the I/O slot with a DS3 Interface card.
2	Ensure DS3 interface circuit packs are firmly pushed into the backplane of the shelf.
3	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
BNC I/O card 1 missing,
BNC I/O card 2 missing,
BNC I/O card 3 missing

Probable cause

The first, second, or third DS3 I/O card is missing.

Note: For information on I/O card slot associations, see “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Insert a DS3 I/o card into the slot.
2	Ensure the DS3 I/O cards are firmly pushed into the backplane of the shelf, and screwed down.
3	If the DS3 I/O cards are firmly seated and the BNC I/O card missing alarm does not clear, check for other more severe alarms and clear them using the appropriate procedures in this document.
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
Circuit pack fail

Probable cause

The DS3/STS mapper has failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C,SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the defective unit. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C, for replacement instructions.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
Circuit pack mismatch

Probable cause

The circuit pack in the slot does not match the provisioned type.

Impact

In an unprotected configuration, this is a critical, service-affecting (C,SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
Circuit pack missing

Probable cause

A provisioned slot does not contain a DS3/STS mapper circuit pack.

Impact

In an unprotected configuration, this is a critical, service-affecting (C,SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

If the circuit pack is present in the slot, ensure that it is properly seated.

If the circuit pack is properly seated and the alarm is still raised, replace the DS3/STS mapper as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If the slot is empty, and the DS3 service is no longer provisioned, the alarm can be cleared by taking the DS3 facility and equipment out-of-service. The facilities and equipment are deleted from the host switch.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
Forced switch

Probable cause

A forced switch command has been requested for the DS3/STS Mapper circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Note: An EQP606 log is generated each time protection activity occurs.

Action

Since a test or maintenance action is being performed, no action is required. This alarm point serves as a reminder not to leave a potentially service-affecting condition on the system (especially with live traffic).

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
Lockout request

Probable cause

A lockout command has been issued for the DS3/STS Mapper circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Note: An EQP606 log is generated each time protection activity occurs.

Action

If a test or maintenance action is being performed, no action is required. This alarm point serves as a reminder not to leave a potentially service-affecting condition on the system (especially with live traffic).

If you want to release the manual switch request, follow this procedure.

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr**↵ *The protection switching screen appears.*
2	Display the detailed protection screen: **dtlprot ds3**↵ *The detailed protection screen appears.*
3	Release the lockout: **lockout re < group >**↵ **y**↵ where < group > number of the circuit pack group: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15 for values. *The screen displays a period (.) in the* `Lockout` *column for the corresponding group.*
4	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Eqp DS3
Manual switch request

Probable cause

A manual switch command has been requested for the DS3/STS Mapper circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Note: An EQP606 log is generated each time protection activity occurs.

Action

Since a test or maintenance action is being performed, no action is required. This alarm point serves as a reminder not to leave a potentially service-affecting condition on the system (especially with live traffic).

If you want to release the manual switch request, follow this procedure.

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr**↵ *The protection switching screen appears.*
2	Display the detailed protection screen: **dtlprot ds3**↵ *The detailed protection screen appears.*
3	Release the manual switch: **manual re < group >**↵ **y**↵ where < group > number of the circuit pack group: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15 for values. *The screen displays a period (.) in the* `Manual` *column for the corresponding group.*
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
Protection path fail

Probable cause

The protection switch exerciser failed while attempting to bridge traffic to the protection circuit pack. This indicates that a hardware failure exists on the DS3 protection path. If a DS3 working circuit pack requires protection and a failure exists on the protection path, this alarm is raised as a major alarm since traffic is lost. If no protection is required, the unprotected severity is minor.

Impact

In an unprotected configuration, this is a major service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

To clear the alarm, perform the following step-by-step procedure.

Step	Action
1	Display the DS3 protection equipment screen: **eq ds3 p** ↵ *The DS3 protection equipment screen appears.*

If the equipment state is	Then
IS Trbl	go to step 2
OOS	go to step 3
IS	go to step 10

2	Replace the defective or missing card as indicated in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C. Go to step 4.
3	Change the operating state to IS (in service): **chgstate is** ↵ *The operating state of the protection group changes to IS.*

—continued—

Eqp DS3
Protection path fail (continued)

Step	Action

4 Run the DS3 exciser:

eq sh ↵
exercise ↵

If the alarm	Then
is cleared	end this procedure
is not cleared	go to step 5

5 Verify the state of the *Maintenance* Interface circuit pack:

eq mic ↵

If the MIC state is	Then
anything other than IS	go to step 6
IS	go to step 10

6 Change the state of the MIC to out-of-service:

chgstate oos↵
y↵

7 Perform an out-of-service diagnostic test on the MIC.

Note: Refer to the procedure “Performing a manual diagnostic test” on page 8-10, then return to this point.

If the test	Then
passes	From the MIC equipment screen, change the state of the MIC to in service: **chgstate is**↵ *The state of the MIC changes to IS.* Go to step 9.
fails	go to step 8

8 Replace the MIC as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C, then return here.

9 Run the DS3 exciser:

eq sh ↵
exercise ↵

If the alarm	Then
is cleared	end of procedure
is not cleared	go to step 10

—continued—

Eqp DS3
Protection path fail (continued)

Step	Action

10 Replace the DS3 switcher as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

11 Run the DS3 exerciser:

eq sh ↵
exercise ↵

If the alarm	Then
is cleared	end of procedure
is not cleared	go to step 12

12 Replace the DS3 protection mapper as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

13 Run the DS3 exerciser:

eq sh ↵
exercise ↵

If the alarm	Then
is cleared	end of procedure
is not cleared	go to step 14

14 Verify the state of the active OC-3/OC-12 circuit pack in the Rx direction.

pr; dtlprot <service type> ↵

where

<service type> type of optical service: **oc3** or **oc12**

Verify the state of the optical circuit pack that has its Rx traffic set to On.

If the optics state is	Then
other than IS	go to step 15
IS	end of procedure

15 Replace the optics circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

16 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
Protection switch complete

Probable cause

A DS3/STS Mapper is switched on the standby unit (caused by a manual, automatic or forced switch).

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Note: An EQP606 log is generated each time protection activity occurs.

Action

Step	Action
1	Find out if the switch was automatic or manual. **pr** ↵ **dtlprot ds3** ↵ *The DS3 Protection screen appears. An asterisk * under the `Manual` or `Forced` heading indicates that protection switching is in effect.*

If the protection switch is	Then
manual or forced	the DS3/STS mapper is assumed to be under test. End the procedure.
automatic	go to step 2

Step	Action
2	Check if there are any active DS3/STS mapper alarms raised: **alarms** ↵ **filter eq** ↵

If there are	Then
DS3/STS mapper alarms	clear the alarms using the appropriate procedures in this document.
no DS3/STS mapper alarms	go to step 3

—continued—

Eqp DS3
Protection switch complete (continued)

Step	Action
3	If the cause of the switch is still unknown, ensure that the DS3 facility parameters have been correctly provisioned. **facility ds3 <circuit pack> <port #>** ↵ where <circuit pack> is **p**, **g1** for OC-3; **p**, **g1** to **g4** for OC-12 <port #> is **1** to **3** *The DS3 Facility screen appears.*

If the DS3 parameters are	Then
correct	go to step 4
incorrect	correct the parameters using the procedure for provisioning DS3 facility parameters in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B.

4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
Protection switch fail

Probable cause

Traffic failed to switch from a working DS3/STS mapper to the protection mapper, as a result of an automatic switch, a forced switch or a manual switch.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Check that there are no lockouts in effect: **eq ds3 all** ↵ **dtlprot** ↵
2	Is there an asterisk (*) in the Lockout column?

If	Then
no	go to step 3
yes	go to step 5

Step	Action
3	Is the operating state of the protection mapper IS? **eq ds3 p** ↵

If	Then
no	go to step 4
yes	go to step 6

—continued—

Eqp DS3
Protection switch fail (continued)

Step	Action
4	Display the alarm screen and check for other more severe DS3 protection equipment alarms or MIC equipment alarms. **alarms** ↵

If	Then
another DS3 equipment alarm appears	look up the alarm in this chapter and proceed accordingly
a MIC equipment alarm appears	look up the alarm in this chapter and proceed accordingly
no other more severe alarms appear	go to step 6

5 Release the lockout:

lockout re <circuit pack> ↵

yes ↵

where

<circuit pack> **g1** for OC-3 system, **g1** to **g4**, for OC-12 system

The screen displays a period (.) in the Lockout column for the corresponding group.

—continued—

Eqp DS3
Protection switch fail (continued)

Step	Action
6	Verify the state of the maintenance interface card. Enter the following command on the network element user interface keyboard: **eq mic**↵

If the MIC state is	Then
IS	go to step 7
other than IS	go to step 8

7	Change the state of the MIC to out-of-service: **chgstate oos**↵ **y**↵
8	Perform an out-of-service diagnostic test on the MIC. ***Note:*** Refer to the procedure “Performing a manual diagnostic test” on page 8-10, then return to this point in the procedure.

If the test	Then
passes	go to step 10
fails	go to step 9

9	Replace the MIC as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C, then return here. Go to step 11.
10	From the MIC equipment screen, change the state of the MIC to in service: **chgstate is**↵ *The state of the MIC changes to IS.*
11	Replace the protection DS3/STS Mapper, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
12	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
STS1 intercard fail

Probable cause

A parity error is detected at the backplane between a DS3/STS mapper and an OC-3/OC-12 circuit pack. The cause of this problem may be at the signal source, at the signal destination, or on the signal path.

Impact

In an unprotected configuration, if a parity error is detected between an active OC-3/OC-12 circuit pack and a DS3/STS mapper, this is a critical, service-affecting (C, SA) alarm.

In an unprotected configuration, if a parity error is detected between an inactive OC-3/OC-12 circuit pack and a DS3/STS mapper, this is a minor, not service-affecting (m, nsa) alarm.

In a protected configuration, or, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Display the detailed alarm information for this alarm. *The Detailed Alarm Report screen appears.*
2	From the Detailed Alarm Reports screen, record the slot numbers of the primary and secondary circuit packs. ***Note:*** The primary and secondary slot numbers refer to circuit packs on the common-equipment shelf. The PEC for the primary and secondary circuit packs may not be shown on the screen.
3	Replace the card that occupies the primary slot number, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	the card that you replaced is faulty. End the procedure.
persists	go to step 4

—continued—

Eqp DS3
STS1 intercard fail (continued)

Step	Action
4	Replace the card that occupies the secondary slot number, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	the card that you replaced is faulty. End the procedure.
persists	go to step 5.

5	If there is a problem with the backplane. Contact your next level of support for assistance.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
Switcher circuit pack mismatch

Probable cause

The circuit pack inserted into the shelf does not match the provisioning circuit pack type, which should be a DS3 switcher.

Impact

If a DS3 protection switch is attempted during the mismatch, this is a critical, service-affecting (C, SA) alarm.

If no DS3 protection switches are attempted during the mismatch, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched card with a DS3 Switcher card. See *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
Switcher circuit pack missing

Probable cause

The DS3 Switcher circuit pack is missing.

Impact

If a DS3 protection switch is attempted, this is a critical, service-affecting (C, SA) alarm.

If no DS3 protection switches are attempted, this is a minor, not service-affecting (m, nsa) alarm.

Action

If the slot is empty, insert a DS3 Switcher card in the empty slot. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If there is a DS3 Switcher card in the slot, ensure it is properly seated. If the Switcher circuit pack missing alarm does not clear after re-seating the card, replace the DS3 Switcher card. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
Traffic problem detected

Probable cause

A facility or equipment problem exists, but the system is unable to determine the exact cause of the problem. A DS3 protection bridge operation could not be performed between the working DS3/STS mapper and the protection DS3/STS mapper. This alarm can be caused by any of the following conditions:

- the protection DS3 is already protecting another DS3 circuit pack group
- the protection group is locked out
- the protection DS3/STS mapper is missing
- the DS3 switcher circuit pack is missing
- the MIC is missing
- the DS3/STS mapper is faulty
- the DS3 signal is faulty

Impact

In an unprotected configuration, this is a major, service-affecting (M,SA) alarm.

In a protected configuration, this ia a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Display the DS3 protection screen: **pr** ↵ **dtlprot ds3** ↵ *The DS3 detailed protection screen appears.*

—continued—

Eqp DS3
Traffic problem detected (continued)

Step	Action
2	Check for an active protection event against one of the working DS3 groups. Do this by looking for an asterisk (*) beside any of the DS3 groups, under the headings Forced, AutoSw, or Manual.

If	Then
a Manual or Forced switch is active	Release the protection switch, and this alarm should clear the next time the system attempts a protection bridge.
an AutoSwitch is active	Fix the problem that caused the switch to occur, by diagnosing the DS3 mapper and replacing if need be. Then switch back to the working DS3 mapper. This alarm should clear the next time the system attempts a protection bridge.
there are no active protection switches	go to step 3

Step	Action
3	From the same screen as in step 2, check for a lockout against the protection DS3 mapper. Do this by looking for an asterisk (*) beside the P (protection) group, under the Lockout column.

If	Then
the protection mapper is locked out	Release the lockout: **lockout re <group>** ↵ **y**↵ where <group> is the number of the circuit pack group see. This alarm should clear the next time the system attempts a protection bridge.
the protection mapper is not locked out	go to step 4

Step	Action
4	Ensure that a protection DS3/STS mapper is properly installed in slot 1 of the common-equipment shelf, and that the Active LED is illuminated.
5	If the DS3/STS mapper is properly seated but is not currently active, and traffic hasn't switched to the protection mapper, then service may be lost. Force a switch to the protection mapper. If there is no protection mapper, replace the DS3/STS mapper.
6	Ensure that the DS3 Switcher circuit pack is properly installed in slot 2 of the common-equipment shelf (if it appears as equipped, then it is properly installed, if not replace it).

—continued—

Eqp DS3
Traffic problem detected (continued)

Step	Action
7	Ensure that the maintenance interface card (MIC) is properly installed in the common-equipment shelf, and that the Active LED is illuminated.
8	Replace the DS3/STS mapper that raised this alarm, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
9	If none of the above actions clears this alarm, check the DS3 signal associated with the DS3/STS mapper that raised this alarm.
10	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DS3
VT connection provisioning mismatch

Probable cause

A VT connection is pre-provisioned at a network element that is already equipped with a DS3/STS circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Delete the preprovisioned VT connection. See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B, for instructions. Otherwise, replace the DS3/STS mapper with a DS1/VT mapper circuit pack.

—end—

Eqp DTAP
Circuit pack fail

Probable cause

The digital test access pair (DTAP) failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the DTAP as outlined in *Installing or Replacing the Digital Test Access Pair.*

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DTAP
Circuit pack mismatch

Probable cause

The circuit pack in the slot designated for the digital test access pair does not match the provisioned circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Installing or Replacing the Digital Test Access Pair.*

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DTAP
Circuit pack missing

Probable cause

The digital test access pair is missing from its designated slot.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

If the circuit pack is present in the slot, ensure that it is properly seated.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If the card is properly inserted but still missing, replace the DTAP as outlined in *Installing or Replacing the Digital Test Access Pair.*

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp DTAP
Circuit pack partial fail

Probable cause

Circuit 1 or circuit 2 on the digital test access pair is missing or failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the DTAP as outlined in *Installing or Replacing the Digital Test Access Pair.*

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ESI
End VCO range

Probable cause

The Stratum-3, voltage controlled oscillator (VCO) on the external synchronization interface (ESI) has exceeded 3/4 of its adjustment range.

Impact

This is a warning, not service-affecting (w, nsa) alarm. The clock may be unable to track changes to the external timing reference. The state of the ESI changes to partial fail (PF).

Action

Replace the circuit pack as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ESI
Equipment forced switch request

Probable cause

A forced switch was requested for the working external synchronization interface (ESI).

Impact

This is a minor, not service-affecting (m, nsa) alarm. The alarm clears when the forced switch is cleared. If the forced switch request is not cleared, the protection unit is not available for use by the system in the event of a problem with the working ESI.

Action

When you want to release the forced switch request, follow the procedure below.

Step	Action
1	From the network element status screen, display the ESI Protection screen: **pr;dtlprot esi**↵
2	Release the forced switch request: **force re < group >**↵ **y**↵ where < group > number of the ESI group: **g1** or **g2**
3	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Eqp ESI
Equipment lockout request

Probable cause

An ESI circuit pack has been locked out from performing a protection switch. This alarm serves as a reminder not to leave a potentially service-affecting condition on the system.

Impact

This is a minor, not service-affecting (m, nsa) alarm. The alarm clears when the lockout is cleared.

Action

No action is required unless you want to release the lockout request.

Step	Action
1	From the network element status screen, display the ESI Protection screen: **pr;dtlprot esi**↵ *The ESI Protection screen appears.*
2	Release the lockout request: **lockout re < group >**↵ **y**↵ where < group > number of the ESI group: **g1** or **g2**
3	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Eqp ESI
Equipment manual switch request

Probable cause

The manual protection switch command was requested for the working external synchronization interface (ESI).

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

No action is required. If you want to release the protection switch, follow this procedure.

Step	Action
1	From the network element status screen, display the ESI Protection screen: **pr;dtlprot esi**↵ *The ESI Protection screen appears.*
2	Release the manual switch request: **manual re < group >**↵ **y**↵ where < group > number of the ESI group: **g1** or **g2**
3	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Eqp ESI
Equipment protection switch complete

Probable Cause

A switch from the working external synchronization interface (ESI) to the protection ESI was successfully completed.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Check to see if the protection switch is the result of a manual or forced switch request for maintenance purposes, or if the system automatically switched service to the protection ESI.

Step	Action
1	From the network element status screen, display the ESI Protection screen: **pr;dtlprot esi↵** *The system displays a list of information about the ESI circuit pack.*

If there is an asterisk (*) beside	Then
Forced or Manual	A protection switch was requested. End procedure here.
Automatic	go to step 2

2	Replace the faulty ESI circuit pack as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.
3	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ESI
Equipment protection switch fail

Probable cause

One or both of the external synchronization interfaces failed or is missing, which caused the protection switch to fail.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Check for a higher order alarm against ESI equipment.

Step	Action
1	From any screen, display the list of alarms: **alarms**↵ *A list of alarms appears.*
2	Look for one of the following ESI equipment alarms:

If the alarm is	Then
Subunit fail	go to page 3-149
Subunit mismatch	go to page 3-150
Subunit missing	go to page 3-151
none of the above	retry the protection switch

3	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ESI
Failure to lock

Probable cause

The external synchronization interface (ESI) card failed to lock onto a valid reference. This alarm occurs if the ESI card is unable to synchronize to the timing reference (acquire mode) after 140 seconds.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

If both ESI cards in the ESI carrier raise this alarm, check the timing source.

If one ESI card raises this alarm, replace the ESI circuit pack.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ESI
Intercard failure

Probable cause

The OC-12 unit detected that it is no longer receiving a 51-MHz clock reference from the ESI unit.

Impact

This is a major, service-affecting (M, SA) alarm, (protectable).
This is a minor, not service-affecting (m, nsa) alarm, (unprotectable).

Action

Step	Action
1	Clear all other alarms against OC-12 according to the appropriate alarm and trouble clearing procedures in this document. Ensure that the protected system is working (that is, the traffic in both directions).
2	Replace the ESI circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
3	If the problem persists, replace the OC-12 circuit pack.
4	If the problem continues to persist, contact your next level of support.

—end—

Eqp ESI
Subunit fail

Probable cause

The external synchronization interface card failed.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Note: If the network element system clock source is not set to ESI, this alarm is always raised as a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ESI
Subunit mismatch

Probable cause

The circuit pack in the slot designated for the external synchronization carrier does not match the provisioned circuit pack.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

> ***Note:*** If the network element system clock source is not set to ESI, this alarm is always raised as a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ESI
Subunit missing

Probable cause

A provisioned slot in the external synchronization carrier does not contain an external synchronization interface.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

> ***Note:*** If the network element system clock source is not set to ESI, this alarm is always raised as a minor, not service-affecting (m, nsa) alarm.

Action

If the circuit pack is present in the slot, ensure that it is properly seated.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ESI
Timing generation entry to acquire

Probable cause

The external synchronization interface (ESI) is in acquisition (acquire) mode. The ESI is in the process of locking to the synchronization reference. This mode is typically present on powerup or system reset, until synchronization is achieved.

Impact

This is a warning, not service-affecting (w, nsa) alarm for information only.

Action

No action required. This mode is a transient state that occurs while the ESI subunit circuit pack is tracking to its reference. This typically occurs on power-up or system reset.

A “Failure to lock” alarm is raised if the ESI subunit circuit pack remains in acquire mode as the result of failing to track its reference.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ESI
Timing generation entry to fast

Probable cause

The external synchronization interface (ESI) is in fast acquisition mode. The ESI is adjusting to changes in the reference signal.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

No action required. The ESI is attempting to reacquire synchronization and is adjusting to changes with the external timing reference. The alarm is raised as soon as the ESI enters the fast mode and clears when the ESI frequency has adjusted to the reference input frequency.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ESI
Timing generation entry to freerun

Probable cause

The external synchronization interface (ESI) is in freerun mode (running off its own clock). The ESI is unable to lock to an external timing reference, or the ESI target filter mode is provisioned for Freerun. The voltage controlled oscillator (VCO) is set at the midpoint and is providing a stratum 3 clock. This mode is typically used during installation of the ESI.

Impact

This is a warning, not service-affecting (w, nsa) alarm for information only.

Action

Check to see if the freerun mode is a result of a manual request or the loss of the reference signal.

Step	Action
1	From the Network Element Status screen, display the ESI equipment screen: **eq esi < group >**↵ where < group > the ESI group number: **g1** or **g2** *The ESI equipment screen appears.*
2	Check the setting of the target filter mode as indicated on the screen.

If target filter mode is	Then
freerun	go to step 3
normal or holdover	go to step 5

3

If target filter mode	Then
was intentionally set at freerun mode	no action is required; end the procedure.
was inadvertently set at freerun mode	go to step 4

—continued—

Eqp ESI
Timing generation entry to freerun (continued)

Step	Action

4 Change the target filter mode to normal:

edittarg normal ↵

If the alarm clears, end the procedure here.

If the alarm persists, go to step 5.

5 Check the signal at the source, DSX cross-connect, and at the side interconnect left connector labelled *Ext Sync IF* (see table below), for loss of signal, loss of frame, excessive bipolar violations, or an alarm indication signal.

External synchronization cable pair color coding and pin-out details.

Signal	Pin	Color
Primary reference input (Tip)	1	W 1BL
Secondary reference input (Tip)	3	W 1O
DS1 output (Tip), top ESI	5	W 1G
DS1 output (Tip), bottom ESI	7	W 1BR
Primary reference input (Ring)	14	BL 1W
Secondary reference input (Ring)	16	O 1W
DS1 output (Ring), top ESI	18	G 1W
DS1 output (Ring), bottom ESI	20	BR 1W
Note: All other pins are not used, and are grounded to the frame		

Note: If the signal format is BITSDS1, a DS1 test set may be used to check the signal.
If the signal format is BITSCC (composite clock), an oscilloscope may be used to check the signal.

6 If the signal is present at the source but not at the DSX cross-connect, the cable from the source of the DSX cross-connect appears to be faulty. Repair as required.

If the signal is present at the DSX cross-connect but not at the side interconnect left connector, the ESI cable appears to be faulty. Repair as required.

7 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ESI
Timing generation entry to holdover

Probable cause

The external synchronization interface (ESI) is in holdover mode due to a manual request, or as the result of a loss of the reference signal. (Holdover means the ESI maintains its synchronization based on the last good reference signal).

Note: Timing stability is maintained within 0.37 ppm in ESI holdover mode for 24 hours. Although timing stability is guaranteed to within 4.6 ppm after this period, the ESI timing remains in holdover mode until the reference signal is restored. Therefore the "Timing generation entry to freerun" alarm is not raised.

Impact

This is a warning, not service-affecting (w, nsa) alarm for information only.

Action

Check to see if the holdover mode is a result of a manual request or the loss of the reference signal.

Step	Action
1	From the Network Element Status screen, display the ESI equipment screen: **eq esi < group >**↵ where < group > the ESI group number: **g1** or **g2**

—continued—

Eqp ESI
Timing generation entry to holdover (continued)

Step	Action
	The ESI equipment screen appears.
2	Check the setting of the target filter mode as indicated on the screen.

If target filter mode is	Then
holdover	go to step 3
normal or freerun	go to step 5

3

If target filter mode was	Then
intentionally set at holdover mode	end the procedure
inadvertently set at holdover mode	go to step 4

4 Change the target filter mode to normal:

edittarg normal ↵

If the alarm clears, end the procedure here.

If the alarm persists, go to step 5.

5 Check the signal at the source, DSX cross-connect, and at the side interconnect left connector labelled *Ext Sync IF* (see table below), for loss of signal, loss of frame, excessive bipolar violations, or an alarm indication signal.

6 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp IRTU
Circuit pack fail

Probable cause

The integrated remote test unit (IRTU) failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the IRTU as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp IRTU
Circuit pack mismatch

Probable cause

The circuit pack in the slot designated for the integrated remote test unit does not match the provisioned circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp IRTU
Circuit pack missing

Probable cause

The integrated remote test unit is missing from its designated slot.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

If the circuit pack is present in the slot, ensure that it is properly seated.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If the card is properly inserted but still missing, replace the IRTU as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp IRTU
Common circuitry fail

Probable cause

- A diagnostic or calibration of the circuitry common to the IRTU test heads has failed.
- The Public Switching Telecommunications Network (PSTN) is not set for the country you are operating in, North America or Hong Kong.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	From the network element status screen, display the IRTU equipment screen: **eq irtu** ↵
2	Change the state to out-of-service: **chgstate oos** ↵ **y** ↵
3	Perform an out-of-service diagnostic test on the IRTU. Refer to “Performing a manual diagnostic test” on page 8-10 in this document.
4	Verify that the PSTN load is set for the proper country, North America or Hong Kong. **quit all** ↵ *The CI prompt appears.*
5	Open the PSTN CI tool by typing: **pstnci** ↵
6	Query the status of the PSTN load by typing: **qpstn** ↵ *The PSTN tool displays the present status of the system.* `This system is currently configured for North American PSTN.`

If the test	**Then**
passes and the IRTU comes up in service	mark and monitor for another failure. The problem may be heat-related (pack must warm up before failure mode).
fails	go to step 4

—continued—

Eqp IRTU
Common circuitry fail (continued)

Step	Action
7	Verify that the PSTN is set for the country in which you are operating.

If the PSTN	Then at the prompt type
is correct	go to step 11
should be North America	**selna**
should be Hong Kong	**selhk**

The PSTN CI displays a warning and asks you to confirm the change.

```
**********WARNING**********

      Changing PSTN compliancy drops all active
      calls and aborts all active line testing.

**************************************************
```

8 Confirm the change by typing:

y ↵

9 Query the status of the PSTN load by typing:

qpstn ↵

The PSTN tool displays the present status of the system.

```
This system is currently configured for Hong Kong PSTN.
```

10 Perform an out-of-service diagnostic test on the IRTU. Refer to “Performing a manual diagnostic test” on page 8-10 in this document.

If the test	**Then**
passes and the IRTU comes up in service	go to step 12
fails	go to step 11

11 Replace the IRTU as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance*, Volume 5, and verify that alarm is now off.

12 Close the PSTN CI tool by typing:

quit ↵

The PSTN CI tool closes and the CI prompt appears.

13 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp IRTU
Software download fail

Probable cause

This alarm is generated for one of the following reasons:

- the IRTU load does not exist on the OPC
- the load file is corrupt
- an error in communications occurred

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Use the lomui command to verify that the IRTU software load exists. At the OPC prompt, type: **lomui query_loads** *A list of all the loads installed on the NE appears.*
2	Does the IRTU software load exist?

If the IRTU software load	**Then**
exists	go to step 3
does not exist	contact your next level of support

Step	Action
3	If the IRTU software load already exists, reload the IRTU software, as outlined in Reboot/Load Manager software procedures in *Commissioning and Testing*, Volume 3.

If the alarm	**Then**
clears	end the procedure here
persists	go to step 4

—continued—

Eqp IRTU
Software download fail (continued)

Step	Action
4	If the IRTU still fails to load, open the event browser tool and check for the possible reason why the software does not load. If you do not know how to do this, see the procedures for logging in to the OPC and opening an OPC tool in *OPC User Interface Description,* 323-3001-301, in *Operations, Administration and Provisioning,* Volume 4A. If you cannot continue after you check the event browser, contact the system administrator to ensure the load is present, is not corrupted, and has been properly installed. (If the load is not present, it must be copied from tape.)
5	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp IRTU
Test head 1 fail

Probable cause

- A diagnostic or calibration of test head 1 on the IRTU has failed.
- The Public Switching Telecommunications Network (PSTN) is not set for the country you are operating in, North America or Hong Kong.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	From the network element status screen, display the IRTU equipment screen: **eq irtu** ↵
2	Change the state to out-of-service: **chgstate oos** ↵ **y** ↵
3	Perform an out-of-service diagnostic test on the IRTU. Refer to "Performing a manual diagnostic test" on page 8-10 in this document.

If the test	**Then**
passes and the IRTU comes up in service	mark and monitor for another failure. The problem may be heat-related (pack must warm up before failure mode).
fails	go to step 4

4	Verify that the PSTN load is set for the proper country, North America or Hong Kong. **quit all** ↵ *The CI prompt appears.*
5	Open the PSTN CI tool by typing: **pstnci** ↵
6	Query the status of the PSTN load by typing: **qpstn** ↵ *The PSTN tool displays the present status of the system.* `This system is currently configured for North American PSTN.`

—continued—

Eqp IRTU
Test head 1 fail (continued)

Step	Action

7 Verify that the PSTN is set for the country in which you are operating.

If the PSTN	Then at the prompt type
is correct	go to step 11
should be North America	**selna**
should be Hong Kong	**selhk**

The PSTN CI displays a warning and asks you to confirm the change.

```
**********WARNING**********

      Changing PSTN compliancy drops all active
      calls and aborts all active line testing.

**************************************************
```

8 Confirm the change by typing:

y ↵

9 Query the status of the PSTN load by typing:

qpstn ↵

The PSTN tool displays the present status of the system.

```
This system is currently configured for Hong Kong PSTN.
```

10 Perform an out-of-service diagnostic test on the IRTU. Refer to “Performing a manual diagnostic test” on page 8-10 in this document.

If the test	**Then**
passes and the IRTU comes up in service	go to step 12
fails	go to step 11

11 Replace the IRTU as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance*, Volume 5C, and verify that alarm is now off.

12 Close the PSTN CI tool by typing:

quit ↵

The PSTN CI tool closes and the CI prompt appears.

13 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp IRTU
Test head 2 fail

Probable cause

- A diagnostic or calibration of test head 2 on the IRTU has failed.
- The PSTN is not set for the country you are operating in, North America or Hong Kong.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	From the network element status screen, display the IRTU equipment screen: **eq irtu** ↵
2	Change the state to out-of-service: **chgstate oos** ↵ **y** ↵
3	Perform an out-of-service diagnostic test on the IRTU. Refer to "Performing a manual diagnostic test" on page 8-10 in this document.

If the test	**Then**
passes and the IRTU comes up in service	mark and monitor for another failure. The problem may be heat-related (pack must warm up before failure mode).
fails	go to step 4

4	Verify that the PSTN load is set for the proper country, North America or Hong Kong. **quit all** ↵ *The CI prompt appears.*
5	Open the PSTN CI tool by typing: **pstnci** ↵
6	Query the status of the PSTN load by typing: **qpstn** ↵ *The PSTN tool displays the present status of the system.* `This system is currently configured for North American PSTN.`

—continued—

Eqp IRTU
Test head 2 fail (continued)

Step	Action

7 Verify that the PSTN is set for the country in which you are operating.

If the PSTN	Then at the prompt type
is correct	go to step 11
should be North America	type **selna**
should be Hong Kong	type **selhk**

The PSTN CI displays a warning and asks you to confirm the change.

```
************************WARNING************************

      Changing PSTN compliancy drops all active
      calls and aborts all active line testing.

*******************************************************
```

8 Confirm the change by typing:

y ↵

9 Query the status of the PSTN load by typing:

qpstn ↵

The PSTN tool displays the present status of the system.

```
This system is currently configured for Hong Kong PSTN.
```

10 Perform an out-of-service diagnostic test on the IRTU. Refer to “Performing a manual diagnostic test” on page 8-10 in this document.

If the test	**Then**
passes and the IRTU comes up in service	go to step 12
fails	go to step 11

11 Replace the IRTU as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, and verify that alarm is now off.

12 Close the PSTN CI tool by typing:

quit ↵

The PSTN CI tool closes and the CI prompt appears.

13 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp ITU
Circuit pack fail
Circuit pack mismatch
Circuit pack missing

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on the following AccessNode Express integrated test unit alarms and the appropriate alarm clearing procedures.

- Circuit pack fail
- Circuit pack mismatch
- Circuit pack missing

—end—

Eqp LC
Line card fail

Probable cause

The system has detected a failed line card.

Impact

This is a minor, service-affecting (m, SA) alarm.

> ***Note:*** The default severity for this alarm is minor, service affecting. However, the severity can be provisioned using the OPC and working at the service-level and the line-card-level. For details, see *Line Card Provisioning Procedures*, 323-3001-315, in *Operations, Administration, and Provisioning,* Volume 4B.

Action

Attempt to recover the failed line card by using the following procedure to run a diagnostic test.

Step	Action
1	Display the active alarms screen by typing: **alarms** ↵ *The active alarm screen appears.*
2	From the detailed alarm screen, determine if this alarm is related to the failure of an Epsilon line card (NT4K65).

If	Then
there is one failed NT4K65 line card	go to 3
all NT4K65 line cards have failed	go to 13
the failed line card is not an NT4K65	go to 14

—continued—

Eqp LC
Line card fail (continued)

Step	Action

3 Check for log LC602 with a log reason of “Line card mismatch.”

If there is	Then
a mismatched line card	replace the mismatched line card with one that is compatible with the provisioning for the slot. For details, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C. End the procedure
no mismatched line card	go to step 4

4 Display the line card equipment screen for the failed line card by entering the appropriate command:

If you are working with a line card	Then go to
for AccessNode (AN) that does not use a virtual line concentrating module (VLCM)	step 4a
for AccessNode Express (ANX) that does not use a virtual line concentrating module (VLCM)	step 4b
for AN or ANX that does use a VLCM	step 4c

a. Enter the following command:

eq lc <CDS #> <LC #>↵

where

<CDS #>	copper-distribution shelf number: **1** to **7**
<LC #>	line card number: **1** to **96**

Note: For Omega 4-wire line cards and Omega 6/8-wire line cards, use the lowest even slot number occupied by the card.

The line card equipment screen for the selected card is displayed.

b. Enter the following command:

eq anxlc <VM #> <slot #>↵

where

<VM #>	ANX shelf number: **1** to **28**
<slot #>	line card slot number: **1** to **48**

Note: For Omega 4-wire line cards, use the upper slot number occupied by the card (multiple of 3).

The line card equipment screen for the selected card is displayed.

—continued—

Eqp LC
Line card fail (continued)

Step	Action

c. Enter the following command:

eq lcmic <VLCM #> <LSG #> <LC #>↵

where

<VLCM #>	VCLM number: **1** to **2**
<CDS #>	line subgroup number on DMS-10NA switch: **0** to **19**
<LC #>	line card slot number on DMS-10NA switch within line subgroup: **0** to **31**

Note: You can also use the “eq lc” command to display the line card equipment screen for a VLCM system.

The line card equipment screen for the selected card is displayed.

5 Change the state of the line card to out-of-service:

chgstate oos↵

yes↵

The state changes to out-of-service (OOS).

6 Start the manual diagnostic test:

diagnose ↵

y↵

Note: Diagnostic failures are reported in log EQP307; passes are reported in log EQP602.

7 To view the log report:

admin nep;logs;open LC↵

If the line card	Then
fails	go to step 8
passes	go to step 10

8 Display the line card equipment screen for the failed line card by entering the appropriate command:

If you are working with a line card	Then go to
for AccessNode (AN) that does not use a virtual line concentrating module (VLCM)	step 8a
for AccessNode Express (ANX) that does not use a virtual line concentrating module (VLCM)	step 8b
for AN or ANX that does use a VLCM	step 8c

—continued—

Eqp LC
Line card fail (continued)

Step	Action

a. Enter the following command:

eq lc <CDS #> <LC #>↵

where

<CDS #>	copper-distribution shelf number: **1** to **7**
<LC #>	line card number: **1** to **96**

Note: For Omega 4-wire line cards and Omega 6/8-wire line cards, use the lowest even slot number occupied by the card.

The line card equipment screen for the selected card is displayed.

b. Enter the following command:

eq anxlc <VM #> <slot #>↵

where

<VM #>	ANX shelf number: **1** to **28**
<slot #>	line card slot number: **1** to **48**

Note: For Omega 4-wire line cards, use the upper slot number occupied by the card (multiple of 3).

The line card equipment screen for the selected card is displayed.

c. Enter the following command:

eq lcmic <VLCM #> <LSG #> <LC #>↵

where

<VLCM #>	VCLM number: **1** to **2**
<CDS #>	line subgroup number on DMS-10NA switch: **0** to **19**
<LC #>	line card slot number on DMS-10NA switch within line subgroup: **0** to **31**

Note: You can also use the “eq lc” command to display the line card equipment screen for a VLCM system.

The line card equipment screen for the selected card is displayed.

9 Reset the line card:

resetlc↵

The line cards hardware is reset and the line card is reloaded if appropriate.

If the reset	Then
fails	go to step 11
passes	go to step 10

—continued—

Eqp LC
Line card fail (continued)

Step	Action
10	Change the state of the line card to in service: **chgstate is**↵

If the Line card fail alarm	Then
clears	end the procedure
persists	go to step 11

Step	Action
11	Replace the failed line card as described in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If the alarm	Then
clears	end the procedure
persists	go to step 12

Step	Action
12	Determine if talk battery to the Epsilon line card is removed by checking log LC602 and log LC300. ***Note:*** If talk battery is removed to an Epsilon line card, the red LED on the card illuminates, log LC602 is issued with reason "Line Card Protection ON detected," and log LC300 is issued a few seconds later with the reason "Line Card Fail."

If talk battery is	Then
removed	contact your next level of support about performing a test for talk battery. End the procedure.
not removed	contact your next level of support for assistance. End the procedure.

Step	Action
13	Check for a break in the talk battery supply to the copper-distribution shelf as follows: **a.** Check if the applicable talk battery breaker on the breaker interface panel (BIP) is in the closed position, which is indicated by the number one (1) at the top of the breaker. **b.** Ensure that the talk battery connectors at the BIP and CDS are properly seated and that the cables are not damaged. **c.** Check the -48 V dc supply to the BIP.

If the alarm	Then
clears	end the procedure
persists	contact your next level of support for assistance. End the procedure.

—continued—

Eqp LC
Line card fail (continued)

Step	Action

14 Display the line card equipment screen for the failed line card failed line card by entering the appropriate command:

If you are working with a line card	Then go to
for AccessNode (AN) that does not use a virtual line concentrating module (VLCM)	step 14a
for AccessNode Express (ANX) that does not use a virtual line concentrating module (VLCM)	step 14b
for AN or ANX that does use a VLCM	step 14c

a. Enter the following command:

eq lc <CDS #> <LC #>↵

where

<CDS #>	copper-distribution shelf number: **1** to **7**
<LC #>	line card number: **1** to **96**

Note: For Omega 4-wire line cards and Omega 6/8-wire line cards, use the lowest even slot number occupied by the card.

The line card equipment screen for the selected card is displayed.

b. Enter the following command:

eq anxlc <VM #> <slot #>↵

where

<VM #>	ANX shelf number: **1** to **28**
<slot #>	line card slot number: **1** to **48**

Note: For Omega 4-wire line cards, use the upper slot number occupied by the card (multiple of 3).

The line card equipment screen for the selected card is displayed.

c. Enter the following command:

eq lcmic <VLCM #> <LSG #> <LC #>↵

where

<VLCM #>	VCLM number: **1** to **2**
<CDS #>	line subgroup number on DMS-10NA switch: **0** to **19**
<LC #>	line card slot number on DMS-10NA switch within line subgroup: **0** to **31**

Note: You can also use the “eq lc” command to display the line card equipment screen for a VLCM system.

The line card equipment screen for the selected card is displayed.

—continued—

Eqp LC
Line card fail (continued)

Step	Action
15	Change the state of the line card to out-of-service: **chgstate oos**↵ **yes**↵ *The state changes to out-of-service (OOS).*
16	Start the manual diagnostic test: **diagnose** ↵ **y**↵ *Diagnostic failures are reported in log EQP322; passes are reported in log EQP609.*
17	To view the log report: **admin nep;logs;open eqp**↵

If the line card	Then
fails	go to step 18
passes	go to step 19

18	Reset the line card: **resetlc**↵ *The line cards hardware is reset and the line card is reloaded if appropriate.*

If the reset	Then
fails	go to step 20
passes	go to step 19

19	Change the state of the line card to in service: **chgstate is**↵

If the Line card fail alarm	Then
clears	end the procedure
persists	go to step 20

20	Replace the failed line card as described in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
21	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp LC
Line card missing

Probable cause

This alarm is raised by either of the following conditions:

- an in-service line card, in a slot provisioned for service, is removed from its slot
- a failed line card, in a slot provisioned for service, is removed from its slot

Impact

This is a minor, service-affecting (m, SA) alarm.

Note: The default severity for this alarm is minor, service affecting. However, the severity can be provisioned using the OPC and working at the service-level and the line-card-level. For details, see *Line Card Provisioning Procedures*, 323-3001-315, in *Operations, Administration, and Provisioning*, Volume 4B.

Action

Step	Action
1	Display the active alarms screen by typing: **alarms** ↵ *The active alarm screen appears.*
2	If the alarmed line cards are local, insert the appropriate line card in the alarmed slot as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
3	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp LC
Loss of power at NT1

Probable cause

The line card detected a loss of power at the subscriber's NT1.

Impact

This is a minor, service-affecting (m, SA) alarm.

Action

Ensure that the subscriber's NT1 is properly connected to its power source as instructed in the NT1 documentation.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp LC
NT1 power status changed

Probable cause

For NT1s with dual power supplies, the line card has detected a failure in one of the power supplies.

Impact

This is a minor, service-affecting (m, SA) alarm.

Action

Check the condition of the power supplies at the subscriber's NT1 as instructed in the NT1 documentation.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp LC
NT1 test mode changed

Probable cause

The NT1 is either under test, or it has been taken out of test mode and put back into service.

Impact

This is a minor, service-affecting (m, SA) alarm.

Action

If a loopback test is being performed on an ISDN channel, no action is required. This alarm is simply a notification of the test.

If the NT1 is in service, no action is required. This alarm is simply a notification of the change from test mode to in-service.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp LC
Sync lost with NT1

Probable cause

There is no longer synchronization between the line card and the NT1.

Impact

This is a minor, service-affecting (m, SA) alarm.

Action

Ensure that the subscriber's NT1 is properly connected and operating as instructed in the NT1 documentation.

If the NT1 appears to be operating normally, reset the NT1 to try and regain synchronization.

> ***Note:*** For information on enabling or disabling this alarm, see *Line Card Testing Procedures*, 323-3001-316, in *Operations, Administration, and Provisioning*, Volume 4B.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp LIC
A-link clock driver fail

Probable cause

One of the following conditions causes this alarm:

- The A-link clock driver on one of the narrowband line interface cards (LIC) in a copper distribution shelf (CDS) line card drawer is faulty.
- The mate to the LIC receiving this alarm has blown a fuse.

Each CDS drawer contains two narrowband LICs. In the left CDS drawer, the two LICs (A and B) are in slot 97 and 98. In the right drawer, the two LICs (C and D) are in slot 99 and 100. LIC A and LIC B are mates, and LIC C and LIC D are mates.

If this alarm occurs because a LIC blows a fuse (LIC A in this example), the following occurs:

- LIC A receives a Circuit pack missing alarm.
- LIC B receives an A-link clock driver fail alarm.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Determine the drawer location (shelf, unit, and slot) of the LIC receiving the A-link clock driver fail alarm.
2	Determine if the LIC or its mate is receiving a Circuit pack missing alarm.

If a Circuit pack missing alarm	Then
is raised against one of the LICs	Replace the LIC with the Circuit pack missing alarm. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
is not raised against one of the LICs	Replace the LIC with the A-link clock driver fail alarm. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

—continued—

Eqp LIC
A-link clock driver fail (continued)

Step	Action

3 Determine if the A-link clock driver fail alarm clears.

If the alarm	Then
clears	Complete the following substeps to reseat the LIC that you did not replace: a Pull the ejector latches of the LIC to unfasten the LIC from the shelf. b Slide the LIC out about 1 inch (25.4 mm) until the LIC disengages from the midplane connector. c Wait at least 20 seconds, then gently slide the LIC back into its slot until the ejector latches come in contact with the front of the CDS drawer frame. Push the latches in toward the LIC to engage the circuit pack with the midplane connector. d Determine that the Circuit pack missing alarm, which was raised when you disengaged the LIC from the midplane connector, clears once the LIC re-engages the midplane connector. Contact your next level of Nortel Networks support if the alarm does not clear. The procedure is finished.
does not clear	The LIC that you replaced in step 2 is not faulty. Complete the following substeps: a Reinsert the LIC that you replaced in step 2. b Replace the other LIC in the CDS drawer. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. Contact your next level of Nortel Networks support if the alarm does not clear.

—end—

Eqp LIC
Circuit pack fail

Probable cause

One of the following conditions causes this alarm:

- The line interface card (LIC) has failed.
- The mate to the LIC receiving this alarm has blown a fuse.

Each CDS drawer contains two narrowband LICs. In the left CDS drawer, the two LICs (A and B) are in slot 97 and 98. In the right drawer, the two LICs (C and D) are in slot 99 and 100. LIC A and LIC B are mates, and LIC C and LIC D are mates.

If this alarm occurs because a LIC blows a fuse (LIC A in this example), the following occurs:

- LIC A receives a Circuit pack missing alarm.
- LIC B receives a Circuit pack fail alarm.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Determine the drawer location (shelf, unit, and slot) of the LIC with the Circuit pack fail alarm.
2	Determine if the LIC or its mate is receiving a Circuit pack missing alarm.

If a circuit pack missing alarm	**Then**
is raised against one of the LICs	Replace the LIC with the Circuit pack missing alarm. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
is not raised against one of the LICs	Go to step 4.

—continued—

Eqp LIC
Circuit pack fail (continued)

Step	Action

3 Determine if the Circuit pack fail alarm clears.

If the alarm	Then
clears	Complete the following substeps to reseat the LIC that you did not replace: a Pull the ejector latches of the LIC to unfasten the LIC from the shelf. b Slide the LIC out about 1 inch (25.4 mm) until the LIC disengages from the midplane connector. c Wait at least 20 seconds, then gently slide the LIC back into its slot until the ejector latches come in contact with the front of the CDS drawer frame. Push the latches in toward the LIC to engage the circuit pack with the midplane connector. d Determine that the Circuit pack missing alarm, which was raised when you disengaged the LIC from the midplane connector, clears once the LIC re-engages the midplane connector. Contact your next level of Nortel Networks support if the alarm does not clear. The procedure is finished.
does not clear	The LIC that you replaced in step 2 is not faulty. Complete the following substeps: a Reinsert the LIC that you replaced in step 2. b Go to step 4.

4 From the network element status screen, display the LIC equipment screen by entering:

eq lic; dtllic <cds #> <group>↵

where

<cds #> CDS housing the LIC: **1** to **7**

<group> the LIC unit number: **A**, **B**, **C** or **D**

The LIC equipment screen appears.

—continued—

Eqp LIC
Circuit pack fail (continued)

Step	Action
5	Change the state of the LIC to out-of-service by entering: **chgstate oos**↵ **y**↵
6	Perform a diagnostic on the LIC. ***Note:*** Refer to the procedure "Performing a manual diagnostic test" on page 8-10, then return to this point in the procedure.

If the test	Then
passes	a Return the LIC to service by entering: **chgstate is** b End the procedure.
fails	Replace the LIC with the Circuit pack fail alarm. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C**.**

7	If you cannot successfully complete this procedure, contact your next level of Nortel Networks support.

—end—

Eqp LIC
Circuit pack mismatch

Probable cause

The circuit pack in the slot designated for the line interface card does not match the provisioned circuit pack. This alarm can also be caused by a LIC with an incorrect vintage.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, or one with the correct vintage, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp LIC
Circuit pack missing

Probable cause

This alarm can be caused by one or more of the following conditions:

- A provisioned line interface card (LIC) is missing from its slot in the line drawer.
- The copper-distribution shelf has lost power due to a tripped CDS breaker on the breaker interface panel.
- Both power converters (CDSP) have been removed from the copper-distribution shelf.
- An access interface cable has been disconnected somewhere between the copper-distribution shelf and the side interconnect right circuit pack. If the cable is disconnected from the CDS A connector, LICs A and C are affected. If the cable is disconnected from the CDS B connector, LICs B and D are affected.

  Note: For the above conditions where there is no power to the CDS or the D-link is down, a "LIC circuit pack missing" alarm is raised for each of the provisioned LICs. If all four LICs are provisioned on the CDS, there will be 2 major LIC alarms and 2 minor LIC alarms.

- A hardware fault on a LIC that results in an A-link clock failure fault or a circuit pack fail fault on the mate LIC in the CDS drawer.
- In some cases a faulty AIC may cause a LIC to appear missing.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

—continued—

Eqp LIC
Circuit pack missing (continued)

Action

Step	Action
1	Display the active alarms screen by typing: **alarms** ↵
2	If the circuit pack is present in the slot, ensure that it is properly seated. If the slot is empty, install a circuit pack bearing the correct product equipment code.
3	Ensure that there are no tripped copper-distribution shelf breakers on the breaker interface panel. Check the breakers labelled “CDS 1" through “CDS 7".
4	Ensure that the power converters (CDSP) are properly installed in the copper-distribution shelf. At least one power converter must be installed for the copper-distribution shelf to operate.
5	Check that the NT4K82 access interface cables are properly connected between the copper-distribution shelf and the side interconnect right circuit pack. Connector “CDS A” and “CDS B” on CDS shelf 1, connect to connectors on the side interconnect right labelled “CDS 1A” and “CDS 1B” respectively. (CDS A corresponds to LIC A and C. CDS B corresponds to LIC B and D.)
6	Check if an A-link clock driver fail alarm or a circuit pack fail alarm is associated with either of the two LICs in the same CDS line drawer.

If there is	Then
an A-link clock driver fail alarm	use the procedure for clearing an A-link clock driver fail alarm on 3-182
a circuit pack fail alarm	use the procedure for clearing a circuit pack fail alarm on page 3-184
no alarm	go to step 7

7	If none of the above actions clears this alarm, check for a faulty AIC.
8	Replace the circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. ***Note:*** The ID PROM on the card may be faulty, which causes this alarm to be raised.
9	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp LIC
D-link interface fail

Probable cause

The system has detected a failure on the D-link between the line interface card (LIC) and the access interface card (AIC). The corresponding AIC has a D-link interface fail warning.

One of the following conditions causes this alarm:

- a LIC, D-link cable, or AIC is faulty.
- The mate to the LIC receiving this alarm has blown a fuse.

Each CDS drawer contains two narrowband LICs. In the left CDS drawer, the two LICs (A and B) are in slot 97 and 98. In the right drawer, the two LICs (C and D) are in slot 99 and 100. LIC A and LIC B are mates, and LIC C and LIC D are mates.

If this alarm occurs because a LIC blows a fuse (LIC A in this example), the following occurs:

- LIC A receives a Circuit pack missing alarm.
- LIC B receives a D-link interface fail alarm.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

If the severity of this alarm is warning, not service-affecting (w, nsa), the problem is probably with the card at the other end of the link.

Action

Step	Action
1	Display the active alarms screen by entering: **alarms** ↵ *The alarm screen appears.*
2	Record the shelf number and unit number of the D-link interface receiving the alarm.

—continued—

Eqp LIC
D-link interface fail (continued)

Step Action

Check for a problem with the mate LIC

3 Complete the instructions in the following table:

If a circuit pack missing alarm	Then
is raised against the LIC or its mate	Replace the LIC with the Circuit pack missing alarm. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C**.** Go to step 4.
is not raised against one of the LICs	Go to step 5.

4 Determine if the D-link interface fail alarm clears.

If the alarm	Then
clears	Complete the following substeps to reseat the LIC that you did not replace: a Pull the ejector latches of the LIC to unfasten the LIC from the shelf. b Slide the LIC out about 1 inch (25.4 mm) until the LIC disengages from the midplane connector. c Wait at least 20 seconds, then gently slide the LIC back into its slot until the ejector latches come in contact with the front of the CDS drawer frame. Push the latches in toward the LIC to engage the circuit pack with the midplane connector. d Determine that the Circuit pack missing alarm, which was raised when you disengaged the LIC from the midplane connector, clears once the LIC re-engages the midplane connector. Contact your next level of Nortel Networks support if the alarm does not clear. The procedure is finished.
does not clear	The LIC that you replaced in step 3 is not faulty. Complete the following substeps: a Reinsert the LIC that you replaced in step 3. b Go to step 5.

—continued—

Eqp LIC
D-link interface fail (continued)

Step	Action
5	At the AccessNode, check that the NT4K82 access interface cables are properly connected between the copper-distribution shelf and the side interconnect right circuit pack. Connector “CDS A” and “CDS B” on CDS shelf 1, connect to connectors on the side interconnect right labelled “CDS 1A” and “CDS 1B” respectively. (CDS A corresponds to LIC A and C. CDS B corresponds to LIC B and D.)
6	If this alarm occurs at a time when the cable has recently been connected (or reconnected), then it is possible that the cause is a bent pin on the cable connector. Before you decide to disconnect a cable to check the pins, you must assess the likelihood that a bent pin is the cause of the alarm, and you must assess the difficulty of accessing the cable. For example, if the alarm occurs at a time when the cable has not recently been connected or reconnected, and if you would have to move a bay out of a line up to access the connectors, you probably would decide not to check for bent pins. Do you want to check for bent pins?

If	Then proceed to
yes	step 7
no	step 15

7	Display the detailed equipment screen for the LIC that is in the left-hand drawer and that is connected to the cable with the failed D-link. Enter: **eq lic** ↵ **dtllic < CDS # > < ID >** ↵ where CDS # — the number of the copper-distribution shelf connected to the failed D-link; enter one of 1 to 7 ID — equipment instance designating the LIC; enter **a** if the cable with the failed D-link connects to “CDS A” connectors; enter **b** if the cable connects to “CDS B” connectors *The detailed LIC Equipment screen appears for the desired unit.*

—continued—

Eqp LIC
D-link interface fail (continued)

Step	Action
8	Is the LIC active or inactive?

If the LIC is	Then proceed to
the primary (active) unit	step 9
the secondary (inactive) unit	step 10

9 Switch activity to change the unit to be diagnosed to a secondary (inactive) status. Enter:

switch ↵

Confirmation is requested.

y ↵

The two LICs exchange primary and secondary status.

10 Display the detailed equipment screen for the LIC that is in the right-hand drawer and that is connected to the cable with the failed D-link. Enter:

eq lic ↵

dtllic < CDS # > < ID > ↵

where

CDS #	the number of the copper-distribution shelf connected to the failed D-link; enter one of 1 to 7
ID	equipment instance designating the LIC; enter **c** if the cable with the failed D-link connects to “CDS A” connectors; enter **d** if the cable connects to “CDS B” connectors

The detailed LIC Equipment screen appears for the desired unit.

11 Is the LIC active or inactive?

If the LIC is	Then proceed to
the primary (active) unit	step 12
the secondary (inactive) unit	step 13

—continued—

Eqp LIC
D-link interface fail (continued)

Step	Action
12	Switch activity to change the unit to be diagnosed to a secondary (inactive) status. Enter: **switch** ↵ *Confirmation is requested.* **y** ↵ *The two LICs exchange primary and secondary status.*
13	Disconnect the cable and check for bent pins. Are there bent pins? **If** — **Then** yes — replace the cable no — reconnect the cable
14	Has the alarm cleared, or is it still persisting? **If** — **Then** the alarm has cleared — you are finished the alarm persists — proceed to step 15
15	From any FWPUI screen, display the list of active alarms: **alarms**↵ *The list of active alarms appears.*

—continued—

Eqp LIC
D-link interface fail (continued)

Step	Action
16	Identify from the list of active alarms, the **D-link interface fail** alarm raised against the AIC, and display the detailed alarm report: **dtlalms < alarm # >**↵ where < alarm # > the alarm report number displayed on screen *The detailed alarm screen appears, showing the shelf and slot number of the card.*
17	Replace the card identified in the previous step, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
18	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Eqp LIC
Inter-plane fail

Probable cause

One of the following conditions causes this alarm:

- The system has detected a failure in the line interface card (LIC) protection circuitry.
- The mate to the LIC receiving this alarm has blown a fuse.

Each CDS drawer contains two narrowband LICs. In the left CDS drawer, the two LICs (A and B) are in slot 97 and 98. In the right drawer, the two LICs (C and D) are in slot 99 and 100. LIC A and LIC B are mates, and LIC C and LIC D are mates.

If this alarm occurs because a LIC blows a fuse (LIC A in this example), the following occurs:

- LIC A receives a Circuit pack missing alarm.
- LIC B receives an Inter-plane fail alarm.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Determine the drawer location (shelf, unit, and slot) of the LIC receiving the Inter-plane fail alarm.
2	Determine if the LIC or its mate is receiving a Circuit pack missing alarm.

If a Circuit pack missing alarm	**Then**
is raised against one of the LICs	Replace the LIC with the Circuit pack missing alarm. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C**.**
is not raised against one of the LICs	Replace the LIC with the Inter-plane fail alarm. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

—continued—

Eqp LIC
Inter-plane fail (continued)

Step	Action

3 Determine if the Inter-plane fail alarm clears.

If the alarm	Then
clears	Complete the following substeps to reseat the LIC that you did not replace: a Pull the ejector latches of the LIC to unfasten the LIC from the shelf. b Slide the LIC out about 1 inch (25.4 mm) until the LIC disengages from the midplane connector. c Wait at least 20 seconds, then gently slide the LIC back into its slot until the ejector latches come in contact with the front of the CDS drawer frame. Push the latches in toward the LIC to engage the circuit pack with the midplane connector. d Determine that the Circuit pack missing alarm, which was raised when you disengaged the LIC from the midplane connector, clears once the LIC re-engages the midplane connector. Contact your next level of Nortel Networks support if the alarm does not clear. The procedure is finished.
does not clear	The LIC that you replaced in step 2 is not faulty. Complete the following substeps: a Reinsert the LIC that you replaced in step 2. b Replace the other LIC in the CDS drawer. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. Contact your next level of Nortel Networks support if the alarm does not clear.

—end—

Eqp LIC
Plane messaging corruption

Probable cause

Line cards detected cyclic redundancy check (CRC) errors in one drawer of a plane.

In some cases, the LIC that this alarm is raised against is not faulty. The fact that one LIC is faulty may cause an alarm to be raised against both LICs in the CDS drawer. The faulty LIC will have a circuit pack missing alarm raised against it.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action

1 Determine the drawer location (shelf, unit, and slot) of the LIC the plane messaging corruption alarm is raised against.

2 Determine if a circuit pack missing alarm is raised against either the LIC with the plane messaging corruption alarm or its mate LIC.

Note: Each CDS drawer contains two narrowband LICs. In the left CDS drawer, the two LICs (A and B) are in slot 97 and 98. In the right drawer, the two LICs (C and D) are in slot 99 and 100. LIC A and B are mates and LIC C and D are mates.

If a circuit pack missing alarm	**Then**
is raised against one of the LICs	Go to step 3.
is not raised against one of the LICs	Go to step 8.

3 Replace the LIC that the circuit pack missing alarm is raised against, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

—continued—

Eqp LIC
Plane messaging corruption (continued)

Step	Action

4 Determine if the plane messaging corruption alarm clears.

If the alarm	Then
clears	Reseat the LIC that was not replaced by performing the following substeps: a Pull the ejector latches of the LIC to unfasten the LIC from the shelf. b Slide the LIC out about 1 inch (25.4 mm) until the LIC disengages from the midplane connector. c Wait at least 20 seconds, then gently slide the LIC back into its slot until the ejector latches come in contact with the front of the CDS drawer frame. Push the latches in toward the LIC to engage the circuit pack with the midplane connector. d Determine that the circuit pack missing alarm which was raised when you disengaged the LIC from the midplane connector clears once the LIC is re-engaged to the midplane connector. Contact your next level of Nortel Networks support if the alarm does not clear. The procedure is finished.
does not clear	Go to step 5.

5 The LIC that you replaced in step 3 is not faulty. Remove the spare LIC and replace it with the original LIC.

6 Replace the other LIC in the CDS drawer. Follow the procedure outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C**.**

—continued—

Eqp LIC
Plane messaging corruption (continued)

Step	Action

7 Determine if the plane messaging corruption alarm clears.

If the alarm	Then
clears	Reseat the LIC that was not replaced by performing the following substeps: a Pull the ejector latches of the LIC to unfasten the LIC from the shelf. b Slide the LIC out about 1 inch (25.4 mm) until the LIC disengages from the midplane connector. c Wait at least 20 seconds, then gently slide the LIC back into its slot until the ejector latches come in contact with the front of the CDS drawer frame. Push the latches in toward the LIC to engage the circuit pack with the midplane connector. d Determine that the circuit pack missing alarm which was raised when you disengaged the LIC from the midplane connector clears once the LIC is re-engaged to the midplane connector. Contact your next level of Nortel Networks support if the alarm does not clear. The procedure is finished.
does not clear	Contact your next level of Nortel Networks support.

8 Replace the access interface card (AIC) in the plane generating the alarm. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If the alarm	Then
clears	end the procedure
persists	contact your next level of Nortel Networks support

—end—

Eqp MIC
Alarm relay fail

Probable cause

The alarm relay on the maintenance interface circuit pack failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Although this alarm does not affect service, it is best to take corrective action immediately, so that in the event of an alarm, the relay will function properly.

Action

Step	Action
1	Replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
Circuit pack fail

Probable cause

The maintenance interface circuit pack failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Although this alarm does not affect service, it is best to take corrective action immediately.

This alarm may cause a corresponding alarm to be raised on the processor circuit pack: either *C-bus-A fail, C-bus-B fail, Degraded master CBIC-A,* or *Degraded master CBIC-B*. Take corrective action for the MIC first, then if the processor alarms persist, correct the fault for the processor.

Action

Replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, then return to this procedure.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
Circuit pack mismatch

Probable cause

The incorrect circuit pack is in the slot designated for the maintenance interface circuit pack. In some cases, due to a hardware fault, this alarm can be raised on a circuit pack bearing the correct product engineering code.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
Circuit pack missing

Probable cause

The maintenance interface circuit pack is missing from its slot, it is improperly seated in the shelf backplane, or a hardware fault is preventing it from being detected.

Impact

This is a major, not service-affecting (m, nsa) alarm.

Action

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If the circuit pack is present in the slot, ensure that it is properly seated.

If the circuit pack is properly seated and this alarm is still raised, then replace the circuit pack as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
E2A input fail

Probable cause

The E2A alarm input on the maintenance interface circuit pack failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Wait 10 minutes for this alarm to clear automatically.
2	If the alarm has not cleared automatically after 10 minutes, replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
3	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
Firmware version mismatch

Probable cause

The maintenance interface card (MIC) has incorrect firmware installed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Note: The steps to clear this alarm require you to download the correct version of the MIC firmware. Read the following cautions and meet the following requirements before you download the firmware.

CAUTION
Firmware download is irreversible
The download process cannot be reversed. After the new firmware is installed, you cannot revert to the old firmware version.

CAUTION
Risk of damage to circuit pack
- To prevent damage to the MIC, observe the following cautions during the download:
  Do not remove the maintenance interface (MIC), processor (PROC), or operations controller (OPC) cards.
- **Do not** perform a shelf restart of any kind.
- **Do not** log out of the network element user interface from which the download command is being run

Failure to observe these cautions could damage the MIC, requiring you to return the MIC to Nortel Networks for repair.

Requirements

You can clear this alarm by logging in to the OPC or logging in to the network element directly affected by the MIC firmware version mismatch. If you log in to the OPC, you must meet the following requirements:

- set up a portable OPC at the network element site. If you do not have a portable OPC, you must set up the primary OPC at the network element site.
- have a userID and password that access the OPC at the admin security level

—continued—

Eqp MIC
Firmware version mismatch (continued)

If you log directly in to the network element, you must meet the following requirements:

- connect a terminal to the network element
- have a userID and password that access the network element at the admin security level

Note: You cannot use the select network element command to clear the alarm, so be sure you log in to the network element directly affected by the firmware version mismatch.

Action

Step	Action
1	From the network element user interface, enter: **quit all** ↵ **micdlci**↵ *The following prompt appears:* micdlci: >
2	Download the MIC firmware by entering: **download**↵ *A message asks you to confirm the download.*
3	At the confirmation message, enter: **yes**↵ *The MIC firmware is retrieved from the OPC and transferred to the MICH, which is then initialized. The process takes about one minute to complete. After the download, the MIC card is reset. This process takes about five minutes. A message displays the status of the download. When the firmware is downloaded, the firmware version mismatch alarm clears.*

—continued—

Eqp MIC
Firmware version mismatch (continued)

Step	Action
4	Wait until the time needed for the download elapses or until the version mismatch alarm clears before you proceed. If the screen displays a message that the download has failed, contact your next level of support.
5	Return to the main network element user interface screen by entering: **quit all**↵ **fwp**↵ *The Network Element Status screen appears.*
6	At the network element user interface, enter: **alarms**↵ *A list of alarms appears for the network element you are logged in to.*

If the alarm	Then
has cleared	you have completed the procedure
has not cleared	contact your next level of support

—end—

Eqp MIC
LED driver fail

Probable cause

The LED driver on the maintenance interface circuit pack failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm. The lamp test is not available while this alarm is raised.

Action

Step	Action
1	Replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
Local craft interface port fail

Probable cause

The local craft interface port on the maintenance interface circuit pack failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm. The DTE and DCE ports are not available for local craft interface while this alarm is raised.

Action

Step	Action
1	From the network element status screen display the MIC equipment screen: **eq mic**↵ *The MIC equipment screen appears.*
2	Change the state of the MIC to out-of-service: **chgstate oos**↵ **y**↵ *The MIC state changes to OOS.*
3	Change the state of the MIC to in-service: **chgstate is**↵ *The MIC state changes to IS.*
4	Display the list of alarms: **alarms**↵

If this alarm	Then
clears	end the procedure here
persists	step 5

Step	Action
5	Reseat the MIC in its slot, then redisplay the list of alarms: **alarms**↵

If this alarm	Then
clears	end the procedure here
persists	step 6

Step	Action
6	Replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
7	If you cannot successfully complete this procedure, contact your next level of support

—end—

Eqp MIC
Non-volatile store fail

Probable cause

The non-volatile store (NVS) on the maintenance interface circuit pack failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Note: If there is a power failure while this alarm is raised, traffic may be lost.

Action

Step	Action
1	Wait 10 minutes for this alarm to clear automatically.
2	If the alarm has not cleared automatically after 10 minutes, replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
3	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
Non-volatile store mismatch

Probable cause

The non-volatile store (NVS) on the maintenance interface circuit pack is mismatched.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Wait 10 minutes for this alarm to clear automatically.
2	If the alarm has not cleared automatically after 10 minutes, replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
3	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
Orderwire fail

Probable cause

The orderwire circuit on the maintenance interface circuit pack failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm. Orderwire is unavailable while this alarm is raised.

Action

Step	Action
1	Wait 10 minutes for this alarm to clear automatically.
2	If the alarm has not cleared automatically after 10 minutes, replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
3	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
Parallel telemetry relay fail

Probable cause

The parallel telemetry relay on the maintenance interface circuit pack failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm. Parallel telemetry output points are unavailable while this alarm is raised.

Action

Step	Action
1	Replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance*, Volume 5C.
2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
Performance monitor clock fail

Probable cause

The performance monitoring (PM) clock on the maintenance interface circuit pack failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm. Performance monitoring is unavailable while this alarm is raised.

Action

Step	Action
1	From the network element status screen display the MIC equipment screen: **eq mic**↵ *The MIC equipment screen appears.*
2	Change the state of the MIC to out-of-service: **chgstate oos**↵ **y**↵ *The MIC state changes to OOS.*
3	Change the state of the MIC to in-service: **chgstate is**↵ *The MIC state changes to IS.*
4	Display the list of alarms: **alarms**↵

If this alarm	Then
clears	end procedure here
persists	step 5

5	Replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
Protection switch relay fail

Probable cause

The protection switching relay on the maintenance interface circuit pack failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm. Protection switching is not available while this alarm is raised. If a protection switch is in effect when this alarm is raised, the protection switch is dropped.

Action

Replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
Serial telemetry port fail

Probable cause

The serial telemetry port on the maintenance interface circuit pack failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm. Serial telemetry is not available while this alarm is raised.

Action

Step	Action
1	From the network element status screen display the MIC equipment screen: **eq mic**↵ *The MIC equipment screen appears.*
2	Change the state of the MIC to out-of-service: **chgstate oos**↵ **y**↵ *The MIC state changes to OOS.*
3	Change the state of the MIC to in-service: **chgstate is**↵ *The MIC state changes to IS.*
4	Display the list of alarms: **alarms**↵

If this alarm	Then
clears	end procedure here
persists	step 5

5	Replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MIC
Time of day clock fail

Probable cause

The time-of-day (TOD) clock on the maintenance interface circuit pack failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm. The stored time of day is not lost.

Action

Step	Action
1	From the network element status screen display the MIC equipment screen: **eq mic**↵ *The MIC equipment screen appears.*
2	Change the state of the MIC to out-of-service: **chgstate oos**↵ **y**↵ *The MIC state changes to OOS.*
3	Change the state of the MIC to in-service: **chgstate is**↵ *The MIC state changes to IS.*
4	Display the list of alarms: **alarms**↵

If this alarm	Then
clears	end procedure here
persists	step 5

5	Replace the maintenance interface circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MLC
Circuit pack fail
Circuit pack mismatch
Circuit pack missing
Partial circuit pack fail

See the *UE9000 Voice OAM&P User Guide* for information on the following Universal Edge 9000 (UE9000) alarms and the appropriate alarm clearing procedures.

The following alarms are associated with the multi-circuit line card (MLC) on the UE9000 shelf:

- Circuit pack fail
- Circuit pack mismatch
- Circuit pack missing
- Partial circuit pack fail

—end—

Eqp MTAC
Circuit pack fail

Probable cause

The metallic test access card failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MTAC
Circuit pack mismatch

Probable cause

The circuit pack in the slot designated for the metallic test access card does not match the provisioned circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp MTAC
Circuit pack missing

Probable cause

The metallic test access card is missing from its designated slot.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

If the circuit pack is present in the slot, ensure that it is properly seated.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC1
Rx line AIS
Rx loss of frame
Rx loss of signal
Rx RFI
Rx signal degrade
Rx signal failure
Rx section trace mismatch

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on these AccessNode Express OC1 shelf processor alarms and the appropriate alarm clearing procedures.

—end—

Eqp OC1

STS1 Rx AIS

STS1 Rx excessive BIP error rate

STS1 Rx loss of pointer

STS1 Rx path trace mismatch

STS1 Rx RFI

STS1 Rx signal degrade

STS1 Rx signal label mismatch

STS1 Rx unequipped

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on these AccessNode Express OC1 shelf processor alarms and the appropriate alarm clearing procedures.

—end—

Eqp OC1

VT Rx AIS

VT Rx excessive BIP error rate

VT Rx loss of pointer

VT Rx RFI

VT Rx signal degrade

VT Rx signal label mismatch

VT Rx unequipped

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on these AccessNode Express OC1 shelf processor alarms and the appropriate alarm clearing procedures.

—end—

Eqp OC-3/OC-12 **Channel match fail**

Probable cause

The G2 (group 2) which is typically the standby OC-3/OC-12 optical interface group failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Follow the instructions in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, to replace the OC-3 (NT7E01) or OC-12 (NT7E02) standby (G2) optical interface. When the standby optical interface has been replaced, return to this procedure.
2	After replacing the standby optical interface, wait 20 seconds, then determine the status of this alarm:

If this alarm	Then
persists	go to step 3
clears	end the procedure

Step	Action
3	For the far-end network element, follow the instructions in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, to replace the OC-3 (NT7E01) or OC-12 (NT7E02) standby (G2) optical interface. When the standby optical interface has been replaced at the far-end network element, return to this procedure.
4	After replacing the standby optical interface at the far-end network element, wait 20 seconds, then determine the status of this alarm:

If this alarm	Then
persists	go to step 5
clears	end the procedure

Step	Action
5	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12 **Circuit pack fail**

Probable cause

The OC-3 or OC-12 optical interface failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the faulty OC-3 or OC-12 interface as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12 **Circuit pack mismatch**

Probable cause

The circuit pack in the slot designated for the OC-3 or OC-12 interface does not match the provisioned circuit pack.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with an OC-3 or OC-12 interface bearing the correct product equipment code, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12 **Circuit pack missing**

Probable cause

A provisioned slot does not contain an OC-3 or OC-12 interface.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

If the circuit pack is present in the slot, ensure that it is properly seated.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Circuit pack reach mismatch

Probable cause

The working and protection OC-3 or OC-12 interfaces installed in the shelf do not have the same reach capabilities (for example, long reach versus intermediate reach).

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched OC-3 or OC-12 interfaces with an optical interface bearing the correct product equipment code, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Entry to SONET clock freerun

Probable cause

The input reference to the system clock is lost, and the network element is in SONET clock freerun mode.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Provision another clock source as shown in the following procedure.

Step	Action
1	From the Network Element Status screen, display the shelf equipment screen: **eq sh** ↵ *The shelf equipment screen appears.*
2	Display the shelf provisioning screen: **edit** ↵ *The shelf equipment provisioning screen appears.*
3	Change the clock source: **clocksrc <source>** ↵ where <source> system clock source: **esi** (for the FCOT), or **looptimed** (for the RFT) *The selected value appears on screen beside the field entitled* `Clock Source`*.*
4	Display the list of active alarms: **alarms** ↵ *The list of active alarms appears.*

—continued—

Eqp OC-3/OC-12
Entry to SONET clock freerun (continued)

Step	Action

5 Determine if the alarm message `Entry to SONET clock freerun`, no longer appears.

If	Then
clears	end this procedure
persists	go to step 6

6 Check the clock source for the input reference to the OC-3/OC-12 system clock.

Note: In an FCOT, the primary OC-3/OC-12 system clock is sourced from the ESI card. In an RFT, the OC-3/OC-12 system clock is sourced from a reference derived from the incoming OC-3/OC-12 fiber.

If the clock source is	Then
present	go to step 7
not present	go to step 8

7 Ensure that there is a proper clock source for the OC-3/OC-12 system clock by correcting any faults or by choosing an alternative system clock source.

8 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Fiber connection error

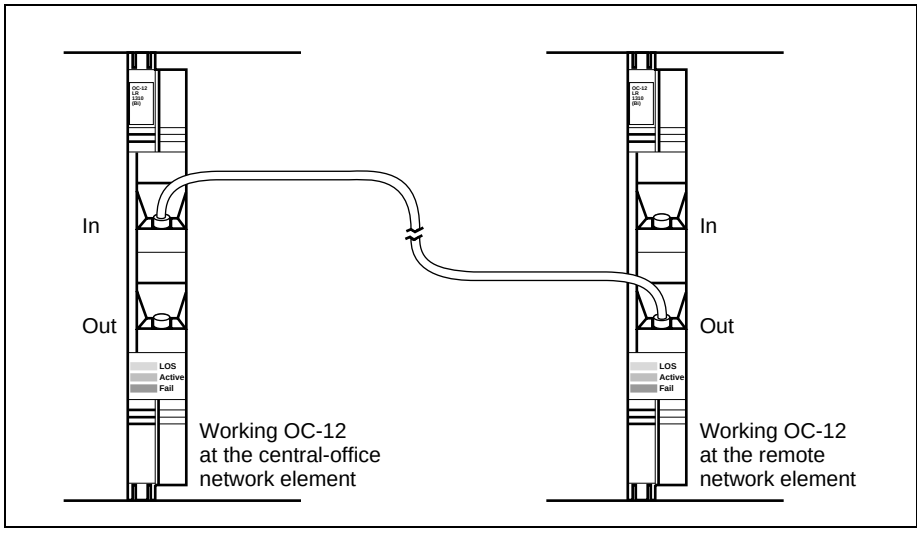
Probable cause

The fiber-optic cable connected to the receiver (Rx) on the working OC-3 or OC-12 interface, is connected to the transmitter (Tx) on the far-end OC-3 or OC-12 protection interface.

Impact

This is a critical, service-affecting (C, SA) alarm. All OC-3 or OC-12 traffic is lost.

Action

Step	Action
1	Verify all origination and termination points for the fiber-optic cables connected to the OC-3 or OC-12 circuit packs. Fibers from the G1 (working) OC-3 or OC-12 at the FCOT must connect to the G1 (working) OC-3 or OC-12 at the RFT. The proper connection is from receiver (Rx) to transmitter (Tx). The following figure shows how the OC-12 Rx at one end, connects to the Tx at the other. Only one connection is shown for clarity. There is a corresponding Tx to Rx connection. PC-10783 

—end—

Eqp OC-3/OC-12 **Firmware version mismatch**

Probable cause

One OC-3 or OC-12 optical interface has different firmware than the other optical interface.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the OC-3 or OC-12 optical interface, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Forced switch request

Probable cause

The forced protection switch command was requested for the working OC-3 or OC-12 optical interface circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Note: An EQP606 log is generated each time protection activity occurs.

Action

No action is required. If you want to release the forced switch, follow this procedure.

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr**↵ *The protection switching screen appears.*
2	Display the detailed protection screen: **dtlprot < optical type >**↵ where < optical type > type of optical interface: **oc3** or **oc12** *The detailed protection screen appears.*
3	Release the forced switch: **forced re < group >**↵ **y**↵

If you have this type of optical circuit pack	Then your <group> number is
OC-3	all, g1, g2, g1s, g2s, g3, g4, g5, g6, g7, or g8
OC-12	all, g1, or g2

The screen displays a period (.) in the `Forced` *column for the corresponding group.*

4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12 **Intercard failure**

Probable cause

A failure has occurred between the OC-3/OC-12 circuit pack and another card. Not enough information is available to fail either card so an intercard alarm is raised.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Display the detailed alarm information for this alarm. *The Detailed Alarm Report screen appears.* ***Note:*** For information on displaying alarm information see “Displaying alarms” on page 1-2.
2	From the Detailed Alarm Reports screen, record the slot numbers of the primary and secondary circuit packs. ***Note:*** The primary and secondary slot numbers refer to circuit packs on the common-equipment shelf. The PEC for the primary and secondary circuit packs may not be shown on the screen.
3	Determine which cards occupy the primary and secondary slots.

If	Then
both cards are OC-3/OC-12	go to step 5
one card is an OC-3/OC-12 card and the other is a DS1/VT or DS3/STS mapper	go to step 4

—continued—

Eqp OC-3/OC-12
Intercard failure (continued)

Step	Action

4 Replace the DS1/VT or DS3/STS mapper as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If this alarm	Then
clears	the card that you replaced is faulty. End the procedure.
persists	replace the OC-3/OC-12 card, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. End the procedure.

5 Display the OC-3/OC-12 detailed protection screen:

pr;dtlprot < type >

where

< type > is the equipment type: **oc12** or **oc3_g1**

The detailed protection screen appears.

6 Check the values under the Tx Rx heading to determine the active and inactive units.

If	Then
one OC-3/OC-12 unit is active and the other unit is inactive	go to step 7
both units are active	go to step 8

7 Replace the inactive OC-3/OC12 circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If this alarm	Then
clears	the card that you replaced is faulty. End the procedure.
persists	replace the other OC-3/OC-12 card, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. End the procedure.

—continued—

Eqp OC-3/OC-12
Intercard failure (continued)

Step	Action
8	Replace the OC-3/OC-12 card in the primary slot as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If this alarm	Then
clears	the card that you replaced is faulty. End the procedure.
persists	replace the OC-3/OC-12 card in the secondary slot as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. End the procedure.

9	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Laser bias current

Probable cause

The laser bias current is no longer within its specified operating range which is required to maintain the laser output.

Impact

This is an warning, not service-affecting (w, nsa) alarm.

Action

If this condition persists or gets worse, replace the OC-12 circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12 **Laser degrade**

Probable cause

The laser on the OC-3 or OC-12 interface is faulty.

Impact

This is a warning, not service-affecting (w, nsa).

Action

Replace the OC-3 or OC-12 interface, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Lockout protection operation fail

Probable cause

A K-byte failure occurred on the lockout protection operation.

Impact

This is a minor, not service-affecting (m, nsa).

Action

Step	Action

CAUTION
Loss of traffic
Do not remove the circuit pack without advice from your Nortel Networks support group.

1 Collect as much information as you can about the events leading to this alarm.

2 Contact your next level of support of your Nortel Networks support group.

—end—

Eqp OC-3/OC-12 **Lockout request**

Probable cause

The lockout command was entered against the working OC-3 or OC-12 interface for maintenance purposes.

Impact

This is a minor, not service-affecting (m, nsa) alarm. The lockout command on OC-3 or OC-12 always brings the traffic back to unit G1 regardless of the impact to traffic. If the OC-3 or OC-12 remains locked out, the system is unable to automatically switch to the unit G2 in the event of a problem.

Note: An EQP606 log is generated each time protection activity occurs.

Action

No action is required. If you want to release the lockout, follow this procedure.

CAUTION
The lockout command supersedes current system status, and will force the optical path onto the G1 optics regardless of the impact to traffic.

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr**↵ *The protection switching screen appears.*
2	Display the detailed protection screen: **dtlprot < optical type >**↵ where < optical type > type of optical interface: **oc3** or **oc12** *The detailed protection screen appears.*
3	Release the lockout: **lockout re** ↵ **y**↵ *The screen displays a period (.) in the* `Lockout` *column for the corresponding group.*
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Manual switch request

Probable cause

The manual protection switch command was requested for the working OC-3 or OC-12 optical interface circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Note: An EQP606 log is generated each time protection activity occurs.

Action

No action is required. If you want to release the manual switch, follow this procedure.

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr**↵ *The protection switching screen appears.*
2	Display the detailed protection screen: **dtlprot< optical type >**↵ where < optical type > type of optical interface: **oc3** or **oc12** *The detailed protection screen appears.*
3	Release the manual switch: **manual re < group >**↵ **y**↵

If you have this type of optical circuit pack	Then your <group> number is
OC-3	all, g1, g2, g1s, g2s, g3, g4, g5, g6, g7, or g8
OC-12	all, g1, or g2

The screen displays a period (.) in the `Manual` *column for the corresponding group.*

4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Protection oscillation control activated

Probable cause

An automatic lockout is in effect.

Impact

This is a minor, not service-affecting (m, nsa) alarm. If the OC-3/OC-12 remains locked out, the system is unable to automatically switch to the protection unit in the event of a problem.

Action

No action is required. However, if you want to release the lockout, follow this procedure.

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr**↵ *The protection switching screen appears.*
2	Display the detailed protection screen: **dtlprot < optical type >**↵ where < optical type > type of optical interface: **oc3** or **oc12** *The detailed protection screen appears.*
3	Release the lockout: **lockout re** ↵ **y**↵ *The screen displays a period (.) in the* `Lockout` *column for the corresponding group.*
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Protection path fail

Probable cause

The exerciser failed to establish an end-to-end protection bridge between a working OC-3 or OC-12 interface and the protection OC-3 or OC-12 interface.

Note: An EQP606 log is generated each time protection activity occurs.

Impact

This is a major, not service-affecting (M, nsa) alarm. While this warning is in effect, service cannot be switched to the protection OC-3 or OC-12 interface in the event of a problem with the working unit.

Action

Step	Action

1 Display the OC-3 or OC-12 equipment screen for the OC-3/OC-12 optical interface that is the standby protection unit:

eq < optical type > < group >↵

If your <optical type> is	Then your <group> number is
OC-3	all, g1, g2, g1s, g2s, g3, g4, g5, g6, g7, or g8
OC-12	all, g1, or g2

Note: The current status (`Active` or `Standby`) of the OC-3/OC-12 optical interface is indicated to the right of the heading `Status:`

The OC-3 or OC-12 equipment screen appears.

If state field indicates	Then
IS - Trbl	go to step 2
OOS	go to step 3
IS	go to step 4

2 Replace the OC-3/OC-12 optical interface as indicated in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. End the procedure here.

Note: The OC-3/OC12 slot number is displayed to the right of the heading `Circuit Packs:`

—continued—

Eqp OC-3/OC-12
Protection path fail (continued)

Step	Action
3	Change the operating state to IS (in service): **chgstate is**↵

If the state is	Then
IS	go to step 4
not IS	Replace the OC-3/OC-12 optical interface as indicated in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. End the procedure.

4 Verify the state of the maintenance interface circuit pack:

eq mic↵

The MIC equipment screen appears.

If the MIC state is	Then
IS-Trbl	go to step 5
IS	go to step 6

5 Replace the MIC as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
End the procedure here.

6 Replace the standby (protection) OC-3 or OC-12 interface, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

7 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Protection scheme mismatch

Probable cause

The OC-3/OC-12 protection scheme at the local area network element does not match the protection scheme at the far-end network element. One network element is provisioned for 1+1 protection, and the other is provisioned for 1:1 protection.

Impact

This is a warning, not service-affecting (w, nsa).

Action

Ensure that the provisioned protection parameters are the same for OC-3/OC-12s at each network element. See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Protection switch complete

Probable cause

Service has been successfully switched from the working OC-3 or OC-12 to the protection OC-3 or OC-12.

Impact

This is a warning, not service-affecting (w, nsa) alarm for information only.

Note: An EQP606 log is generated each time protection activity occurs.

Action

No action is required.

—end—

Eqp OC-3/OC-12
Protection switch fail

Probable cause

A switch from the working OC-3 or OC-12 to the protection OC-3 or OC-12 was unsuccessful.

Impact

This is a critical, service-affecting (C, SA) alarm. Traffic associated with the OC-3 or OC-12 is lost.

Action

Step	Action
1	Check that there are no lockouts in effect: **eq <optical type> all;dtlprot**↵ where < optical type > type of optical interface: **oc3** or **oc12** *The OC-3 or OC-12 protection screen appears.*
2	Is there an asterisk (*) in the Lockout column?

If	Then
no	go to step 3
yes	go to step 5

3 Is each operating state IS Normal?

If	Then
no	go to step 4
yes	go to step 7

—continued—

Eqp OC-3/OC-12
Protection switch fail (continued)

Step	Action

4 Display the alarm screen and check for other more severe OC-3 or OC-12 equipment alarms or MIC equipment alarms.

alarms↵

If	Then
another OC-3 or OC-12 equipment alarm appears	look up the alarm in this chapter and proceed accordingly
no other more severe alarms appear	go to step 7

5 Release the lockout:

lockout re ↵
y↵

The screen displays a period (.) in the `Lockout` *column for the corresponding group.*

6 Perform a manual protection switch to the standby OC-3/OC-12:

manual op < group >

y↵

If your have this type of optical circuit pack	Then your <group> number is
OC-3	all, g1, g2, g1s, g2s, g3, g4, g5, g6, g7, or g8
OC-12	all, g1, or g2

If the protection switch	Then
succeeds	end the procedure
fails	go to step 4

7 Replace the protection OC-3 or OC-12 optical interface as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

8 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Protection switching byte fail/Improper APS code

Probable cause

The G2 (group 2) standby OC-3/OC-12 optical interface failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Follow the instructions in *Module Replacement Procedures*, 323-3001-547, in Maintenance, Volume 5C, to replace the OC-3 (NT7E01) or OC-12 (NT7E02) standby (G2) optical interface. When the standby optical interface has been replaced, return to this procedure.
2	After replacing the standby optical interface, wait 20 seconds, then determine the status of this alarm:

If this alarm	Then
persists	go to step 3
clears	end the procedure

Step	Action
3	For the far-end network element, follow the instructions in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, to replace the OC-3 (NT7E01) or OC-12 (NT7E02) standby (G2) optical interface. When the standby optical interface has been replaced at the far-end network element, return to this procedure.
4	After replacing the standby optical interface at the far-end network element, wait 20 seconds, then determine the status of this alarm:

If this alarm	Then
persists	go to step 5
clears	end the procedure

Step	Action
5	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12 **Receive fail**

Probable cause

The receiver on the OC-3 or OC-12 optical interface failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the OC-3 or OC-12 interface as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12 **STS1 intercard fail**

Probable cause

There is a hardware fault on a an OC-3/OC-12 circuit pack, on a DS1/VT or DS3/STS mapper, or on the backplane. An STS1 signal is not being received properly. The cause of the problem may be at the signal source, at the signal destination or on the signal path.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Display the detailed alarm information for this alarm. *The Detailed Alarm Report screen appears.* ***Note:*** For information on displaying alarm information, see “Displaying alarms” on page 1-2.
2	From the Detailed Alarm Reports screen, record the slot numbers of the primary and secondary circuit packs. ***Note:*** The primary and secondary slot numbers refer to circuit packs on the common-equipment shelf. The PEC for the primary and secondary circuit packs may not be shown on the screen.
3	Replace the card that occupies the primary slot number, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If this alarm	Then
clears	the card that you replaced is faulty. End the procedure.
persists	go to step 4

—continued—

Eqp OC-3/OC-12
STS1 intercard fail (continued)

Step	Action
4	Replace the card that occupies the secondary slot number, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If this alarm	Then
clears	the card that you replaced is faulty. End the procedure.
persists	go to step 5

5	If there is a problem with the backplane, contact your next level of support for assistance.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Switch mode mismatch

Probable Cause

The provisioned protection switching attributes for the central office OC-3 or OC-12 do not match those of the remote OC-3 or OC-12. One is provisioned for unidirectional, and the other is provisioned for bidirectional.

Note: While the mismatch is in effect, the system defaults to unidirectional protection switching.

Impact

This is a warning, not service-affecting (w, nsa) alarm for information only. If a problem occurs with the working OC-3 or OC-12 circuit pack, protection switching will not work.

Action

Check the provisioned protection switch modes at both network elements.

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr.**↵ *The protection switching screen appears.*
2	Display the detailed protection screen: **dtlprot <optical type>** ↵ where < optical type > type of optical interface: **oc3** or **oc12** *The OC-3 or OC-12 detailed protection screen appears.*

—continued—

Eqp OC-3/OC-12
Switch mode mismatch (continued)

Step	Action
3	Display the protection provisioning screen: **protprov**↵ *The protection provisioning screen appears.*
4	Note the switch mode. It will be either unidirectional or bidirectional.
5	Quit from this screen: **quit**↵ *The protection switching screen appears.*
6	Log in to the remote network element and repeat from step 1 for the other network element. If the switch modes are different, see *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B.
7	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Transmission rate mismatch

Probable cause

The transmission rate of the optical circuit pack does not match the transmission rate of the network element (NE). This can be due to an incorrect optical interface installed at the NE, or due to a commissioning error.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

To clear this alarm either replace the current optical interface with one having the correct optical transmission rate, as described in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C, or change the transmission rate commissioned for this network element, as described in the following procedure.

Step	Action
1	Log in to the operations controller (OPC) user interface, and open the Commissioning Manager tool. *The Commissioning Manager main window appears.*
2	Select the **Commission Network Element** button, by pressing Ctrl_A (or Keypad 0). *The Network Element Commissioning Data dialog appears.*
3	Tab to the **Transmission rate** field, and display the chooser menu by pressing Ctrl_L (or Keypad 3).
4	Move to the required rate, and select it by pressing Space (or Keypad 0). *The selected transmission rate appears in the field.*
5	To complete the entry of the transmission rate, for this network element, tab to the **OK** button, and select it by pressing Ctrl_A (or Keypad 0). *The Commissioning Manager main window appears.*
6	Log out of the OPC.
7	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12 **Transmit fail**

Probable cause

The transmitter on the OC-3 or OC-12 interface failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the OC-3 or OC-12 interface as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-3/OC-12
Unable to track clock reference

Probable cause

There is a hardware fault on an OC-3/OC-12 circuit pack.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Replace the OC-3/OC-12 circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-12
Default K bytes

Probable cause

The automatic protection switching (APS) bytes transmitted with the source node ID equal the destination node ID.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Reprovision the circuit pack in the node transmitting the default K-bytes. See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B.
2	If the alarm persists, replace the circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

—end—

Eqp OC-12
Duplicate NE ID Alarm

Probable Cause

The Network Name Service (NNS) software detected a non-unique NE ID in the network. This network element was commissioned using a NE ID number that is not unique throughout the network.

Impact

The non-unique NE ID alarm is minor (M) but also service affecting (SA). Non-unique NE IDs can cause problems with routing and remote login.

Action

Step	Action
1	Contact the next level of technical support.

—end—

Eqp OC-12
Duplicate NE Name

Probable cause

The Network Name Service (NNS) software detected a non-unique NE name in the network. This network element was commissioned using a NE name that is not unique throughout the network. This alarm is not severe enough to lose datacomm traffic on the network.

Impact

The duplicate NE name alarm is a warning (W) level alarm that is non service affecting (NSA).This could cause problems with remote login.

Action

Before starting this procedure, the following requirements must be met.

- be logged in to the network element user interface (NEUI) and at the main menu level
- be familiar with the command conventions for the interface you are using, and procedures for connecting to an NE and for logging into the NEUI. A complete tour of the NEUI is available in *Network Element User Interface Description*, 323-3001-300, in *Operations, Administration, and Provisioning*, Volume 4A.
- a copy of the Commissioning Results Form, located in *Commissioning and Testing*, in Volume 3
- have a copy or copies of your mapper planning worksheets from "Appendix A: Worksheets" in the *Mapper Layouts Planning Guide*, 323-3001-154, in the *Engineering, Configuration, and Ordering Guide*, Volume 1

Step	Action
1	Access the System Administration screen by entering: **admin nep** ↵ *The Network Element Profile screen is displayed.*

—continued—

Eqp OC-12
Duplicate NE Name (continued)

Step	Action
2	Set the NE name by entering: **nename <nename>** ↵ **where** <nename> is an ASCII string of up to 13 characters, with the first character being an alpha character. ***Note 1:*** Enter the NE name inside single quotes ('NE name'), otherwise all the text is converted to uppercase. Enter NE name with single quotes if you include spaces or special characters (?, =). ***Note 2:*** If the NE name is to be used in conjunction with TL1 target identifier (TID) and system identifier (SID), the TL1 TID/SID permissible character set must be followed. This character set includes uppercase or lowercase letters A to Z, numbers 0 to 9, and the special characters: dash, underscore, comma, and period. The special characters cannot be the first character in the name. *A screen appears when the procedure is completed.*
3	Note the completion of this procedure on the Commissioning Results Form. **—end—**

Eqp OC-12
Entry to SONET clock acquire

Probable cause

An OCn card is locking to the synchronization reference. This mode is typically present at power-up or during system reset. This mode lasts until synchronization is achieved.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

No action is necessary.

—end—

Eqp OC-12
Entry to SONET clock freerun

Probable cause

The OC-12 VTBM optical interface circuit pack is in freerun mode. The OC-12 is not able to lock to a timing reference, or the target clock mode is normally provisioned to freerun. The voltage controlled oscillator (VCO) is not locked to a timing reference and is running at its natural frequency.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action

1 Clear any other alarms against OC-12 equipment or facility according to the appropriate alarm and trouble clearing procedures in this document.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 2

2 Verify the integrity of the OC-12 timing reference signal.

3 Verify whether the target clock mode is set on normal by entering:

eq oc12 <circuit pack> ↵

where

<circuit pack> is **g1** or **g2**

4 If required, change the target clock mode by entering:

edittarg <freerun, normal or **holdover>** ↵

The default target clock mode is **normal**.

—end—

Eqp OC-12
Entry to SONET clock holdover

Probable cause

One of the following conditions causes this alarm:

- The system has lost its synchronization reference.
- The target clock mode has been provisioned to holdover.

Holdover mode means the OC-12 VTBM optical interface circuit pack maintains its synchronization based on the last good reference signal.The VCXO clock holds within a certain frequency range of the last lock-in timing reference. When the reference returns, the OC-12 VTBM optical interface circuit pack (NT7E05) enters Acquire mode. After 24 hours in holdover mode, a log is generated indicating that the circuit pack has been in holdover for 24 hours.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Check to see if the holdover mode is a result of a manual request or the loss of the reference signal.

Step	Action
1	Clear any other alarms against OC-12 equipment or facility according to the appropriate alarm and trouble clearing procedures in this document.

If the alarm	**Then**
clears	you have completed the procedure
persists	go to step 2

—continued—

Eqp OC-12
Entry to SONET clock holdover (continued)

Step	Action
2	From the network element status screen, display the OC12 equipment screen by entering: **eq oc12 <circuit pack group>** ↵ where **<circuit pack group>** **g1** or **g2** *The system displays a list of information for the OC-12 circuit pack.* If the information on the screen lists the target clock mode as Holdover and a test or maintenance operation is being performed, no further action is required. If the information on the screen lists the target clock mode as anything other than Holdover, go to step 3.
3	Verify the integrity of the timing reference signal. **—end—**

Eqp OC-12
Fiber loopback

Probable cause

A transmitter fiber has been looped back to the receiver on the same circuit pack.

Impact

This is a critical, service-affecting (C, SA) alarm.

Action

Step	Action
1	Tx and Rx fibers for both working and protection paths must be properly connected to the optical circuit pack and to the fiber patch panel. Rearrange the fibers so that they connect to the proper transmitter and receiver.

—end—

Eqp OC-12
Firmware corrupt

Probable cause

A firmware load running on circuit pack G1 or G2 (slot 9 or 10) is corrupted.

Impact

This is a minor, not service-affecting (m, nsa) alarm (if protectable).
This is a critical, service-affecting (C, SA) alarm (if not protectable).

Action

Step	Action
1	Download the proper firmware release. See the procedure on verifying the firmware load of an OC-12 optical interface circuit pack in *Commissioning and Testing,* Volume 3. ***Note:*** If you do not know which firmware release is required by your system, see OC-3/OC-12 network element detailed ordering equipment codes in *Engineering and Ordering Information*, 323-3001-032, *Engineering, Configuration, and Ordering Guide,* Volume 1.
2	If you cannot download firmware to the circuit pack, replace the circuit pack. See the procedure for replacing the OC-12 optical interface circuit pack, *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
3	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-12
Firmware/software incompatible

Probable cause

The firmware load in the circuit pack is not compatible with the network element software load.

Impact

In an unprotected configuration this is a critical, service-affecting (C, SA) alarm.
In a protected configuration this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action

1 Do the following:

If	Then
the alarm is raised as part of a software upgrade	no user action is required. Complete the software upgrade procedure. See the procedure on verifying the firmware load of an OC-12 optical interface circuit pack in *Commissioning and Testing,* Volume 3.
the alarm is raised but is not part of a software upgrade	download the proper firmware release. See the procedure on verifying the firmware load of an OC-12 ring circuit pack in *Commissioning and Testing,* Volume 3.
you do not know which firmware release is required by your system	see OC-3/OC-12 network element detailed ordering equipment codes in *Engineering and Ordering Information*, 323-3001-032, in *Engineering, Configuration, and Ordering Guide,* Volume 1.
you cannot download the circuit pack	replace the circuit pack. See the procedure for replacing the OC-12 optical interface circuit pack in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

2 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-12
Firmware trap

Probable cause

A trap has occurred on the firmware running on the OC-12 VTBM optical interface circuit pack (NT7E05) and is shown on the HMI port. A transport control subsystem firmware (TCSFW) trap alarm is raised when the VTM firmware traps.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Contact NT support for assistance.

—end—

Eqp OC-12
Intercard serial link fail

Probable cause

The serial link used by the micro-controllers equipped on the circuit packs G1 and G2 (in slots 9 and 10) has failed.

Impact

This is a major, not service-affecting (M, nsa) alarm.

Action

Step	Action
1	Display the detailed alarm information for this alarm. See the procedure for displaying a detailed alarm report in *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C. The signal source and signal destination are indicated by the primary slot and secondary slot number on the detailed alarm screen. *A screen is displayed.*
2	Do the following:

If the alarm is raised against	Then replace
G1 in slot 9	G2 in slot 10
G2 in slot 10	G1 in slot 9

See the appropriate procedure in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

3	If the problem persists, contact your next level of support.

—end—

Eqp OC-12
Invalid neighbor detected

Probable cause

A network element raises this alarm when a neighboring node transmits an invalid automatic protection switch (APS) ID. Each network element in a ring has an assigned APS ID. In addition, each network element keeps a list of the IDs of all other network elements in the ring. The IDs are arranged by their relative position to the network element. The order of the list allows a network element to identify its neighbors.

During the idle state, network elements at each end of each fiber in a ring exchange APS IDs continuously. (The expected detailed alarms screen displays the actual and expected IDs.) If a network element receives an ID that does not match the expected ID, the network element waits for three seconds, then raises this alarm.

One of the following conditions causes this alarm:

- An incorrect node map was downloaded.
- A protection circuit pack group is out of service (OOS) and an OC-12 protection switch is initiated or active. The network element at which the switch is initiated or active raises the alarm. (This condition also raises the ring protection suspended or the ring protection not available alarm.)
- A protection circuit pack group is OOS, and the routine exerciser is run. The network element running the exerciser raises the alarm.
- A protection switch is active, and the protection circuit pack group at an intermediate network element is placed OOS. The network elements on both sides of the OOS protection circuit pack raise the alarm.
- Two fiber pairs were swapped during installation.

Note: The Rx AIS alarm for OC-12 optical interface circuit packs masks this alarm.

Impact

This is a major, not service-affecting (M, nsa) alarm.

—continued—

Eqp OC-12
Invalid neighbor detected (continued)

Action

Step	Action
1	Return the protection circuit pack group to in service (IS).

If the alarm	Then
clears	you have completed the procedure
persists	go to step 2

2	Download valid APS ID numbers by auditing the configuration data for all network elements in the ring. See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 3

3	Check to be sure the two fiber pairs were not swapped during installation. If they are installed incorrectly, reinstall the fiber pairs.

—end—

Eqp OC-12
Lockout protection request

Probable cause

A protection switch has been requested.

Note: This alarm applies to ring configurations only.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Release the lockout by entering: **protectn**↵ **dtlprot oc12**↵ **lockout re p <circuit pack>**↵ where <circuit pack> **g1** or **g2** ***Note:*** Both working and protection units must be provisioned and in service for any protection switching (lockout, forced switch, manual switch) to be completed. **—end—**

Eqp OC-12
Lockout working request

Probable cause

A lockout has been requested.

Note 1: This alarm applies to ring configurations only.

Note 2: This alarm requires no action if a test or maintenance operation is being performed. During testing or maintenance, the alarm serves as a reminder to remove a potentially service-affecting condition from the system (especially when the system is conveying live traffic).

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	If you want to release the lockout, enter: **protectn**↵ **dtlprot oc12**↵ **<circuit pack>** **lockout re w <circuit pack>**↵ where <circuit pack> **g1** or **g2** ***Note:*** Both working and protection units must be provisioned and in service for any protection switching (lockout, forced switch, manual switch) to be completed. **—end—**

Eqp OC-12
Maps invalid

Probable cause

The OC-12 circuit pack does not have a valid node map.

Impact

This is a major, not service-affecting (M, nsa) alarm.

Action

Step	Action

1 Audit the configuration data. See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 2

2 Download firmware to the VTBM circuit pack. See the procedure on verifying the firmware load of an OC-12 interface circuit pack in *Commissioning and Testing,* Volume 3.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 3

3 Replace the optical interface circuit pack. See the appropriate procedure in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 4

4 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-12
Matchnode connection provisioning mismatch

Probable cause

A matched node connection is preprovisioned using a non-STS-1 tributary.

Note: Matchnode connections are possible only on OC-12 rings.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Delete the preprovisioned matched node connection or deprovision the replace the OC-3 with an STS-1 circuit pack.

—end—

Eqp OC-12
NE id mismatch

Probable cause

Three consecutive and identical frames contain a source node (K2 bit 2-4) that

- does not match a neighbor's node id as defined in the destination node's resident ring map, or
- does not map to an entry in the ring node map.

Impact

This is a minor, not service-affecting (m, nsa) alarm (if protectable).
This is a critical, service-affecting (C, SA) alarm (if not protectable).

Action

Step	Action

1 Audit configuration from OPC. See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 2

2 Replace the OC-12 circuit pack against which the alarm has been raised. See *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C, for replacement instructions.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 3

3 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OC-12
Performance monitor clock fail

Probable cause

The one-second clock used for performance monitoring from the MIC card has failed. This could be caused by the failure of either the OC-12 circuit pack or the MIC circuit pack.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action

1 Replace the maintenance interface controller circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 2

2 Replace the OC-12 circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

If	Then
clears	you have completed the procedure
persists	go to step 3

3 If the alarm continues to persist, contact your next level of support.

—end—

Eqp OC-12
Protection switching byte/APS code inconsistent

Probable cause

Over 12 successive frames, starting with the last frame containing previously consistent APS code, no three consecutive frames contain identical APS bytes.

Impact

This is a minor, not service-affecting (m, nsa) alarm (if protectable).
This is a critical, service-affecting (C, SA) alarm (if not protectable).

Action

Step	Action

1 Replace the maintenance interface controller circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 2

2 Replace the OC-12 circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

If	Then
clears	you have completed the procedure
persists	go to step 3

3 If the alarm continues to persist, contact your next level of support.

—end—

Eqp OC-12
Reference input clock fail

Probable cause

A 51 MHz reference clock from the mate OC-12 circuit pack has failed. The faulty clock cannot be determined.

Impact

This is a minor, not service-affecting (m, nsa) alarm (if protectable).
This is a critical, service-affecting (C, SA) alarm (if not protectable).

Action

Step	Action

1 Replace the OC-12 circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 2

2 Replace the mate OC-12 circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 3

3 If the alarm continues to persist, contact your next level of support.

—end—

Eqp OC-12
Ring protection suspended or unavailable

Probable cause

An automatic ring protection switch cannot occur because of one of the following conditions:

- A craftsperson has put the OC-12 ring loopback circuit pack out of service to perform maintenance.
- The OC-12 ring loopback circuit pack has failed.

Note: When the OC-12 ring loopback circuit pack is in service, the green LED is lit.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action

1 Complete the instructions in the following table:

If the OC-12 ring loopback circuit pack is	Then
out of service for maintenance	return the circuit pack to in service after maintenance is complete
out of service and no maintenance is underway	return the circuit pack to in service
in service	check for other alarms that might identify the problem, then clear those alarms

—end—

Eqp OC-12
STS1 intercard fail

Probable cause

A parity error is detected at the backplane at one of the following locations:

- between an OC-3/OC-12 circuit pack and the tributary circuit packs (DS1, DS3, STS-1)
- between the primary transport circuit packs (OC-12/Lbpk) and secondary transport circuit packs (OC-12/Lpbk)

The cause of the problem might be at the signal source, signal destination or on the signal path. This could be due to a hardware fault that exists on the transport circuit pack, the tributary circuit pack, or the backplane.

Impact

This is a critical, service-affecting (C, SA) alarm, if the OC-3/OC-12 circuit pack is active.
This is a minor, not service-affecting (m, nsa) alarm, if the OC-3/OC-12 circuit pack is inactive.

Action

Step	Action
1	Display the detailed alarm information for this alarm. See the procedure for displaying a detailed alarm report in *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C. The signal source and signal destination are indicated by the primary slot and secondary slot number on the detailed alarm screen. *A screen is displayed.*
2	Replace the circuit pack that occupies the primary slot number. See the appropriate procedure in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
3	If the problem persists, replace the circuit pack that occupies the secondary slot number. ***Note:*** If the alarm clears, the circuit pack replaced is the source of the problem. All other circuit packs replaced before this step are functioning properly and need not be returned to NT for repair.
4	If the problem persists, contact your next level of support.

—end—

Eqp OC-12
STS12 ring link parity error

Probable cause

A parity error has occurred on the STS-12 ring link between the G1 and G2 circuit packs.

Impact

This is a minor, not service-affecting (m, nsa) alarm (if protected).
This is a critical, service-affecting (C, SA) alarm (if not protected).

Action

Step	Action

1 Replace the OC-12 circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 2

2 Replace the mate OC-12 circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 3

3 If the alarm continues to persist, contact your next level of support.

—end—

Eqp OC-12
Synchronization clock fail

Probable cause

The 2 kHz synchronization clock input from the master OC-12 circuit pack that sources the clock to the shelf has failed.

Impact

This is a major, not service-affecting (M, nsa) alarm.

Action

Step	Action
1	Replace the OC-12 circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 2

Step	Action
2	Replace the mate OC-12 circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

If the alarm	Then
clears	you have completed the procedure
persists	go to step 3

Step	Action
3	If the alarm continues to persist, contact your next level of support.

—end—

Eqp OC-12
System clock reference fail

Probable cause

The OC-12 unit detected that it is no longer receiving a 51-MHz clock reference from the ESI unit.

Impact

This is a minor, not service-affecting (m, nsa) alarm (if protectable).
This is a critical, service-affecting (C, SA) alarm (if not protectable).

Action

Note: Before replacing a circuit pack, try to clear the alarm by removing and reseating the same circuit pack (see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C), ensuring the circuit pack is protected before removing and reseating it.

Step	Action
1	Change the OC-12 target clock mode to freerun. See in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B.

If	Then
the alarm is cleared	go to step 2
the alarm is not cleared	go to step 3

2	Switch the clock reference back to normal or provisioned reference. End the procedure here.
3	Replace the optical interface circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

—end—

Eqp OC-12
VT connection provisioning mismatch

Probable cause

A VT connection has been provisioned at a NWK-based network element.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Delete the preprovisioned VT connection. See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B, for instructions.

—end—

Eqp OPC
Configuration audit fail

Probable cause

A configuration audit of a ring has detected a discrepancy between the data stored in the Configuration Manager database on the OPC and the data stored on one or more network elements in the OPC span of control. The audit can be either a manual audit (initiated using the OPC Configuration Manager tool) or a scheduled audit.

The alarm is raised after a hold-off period of 1 to 2 minutes. It is cleared automatically 1 to 2 minutes after a successful configuration audit has been performed. You can also manually clear this alarm according to "Manually clearing OPC alarms" on page 1-6. Manually clear the alarm only when the mismatched configuration data has been corrected and a configuration audit successfully run.

Impact

This is a minor, not service-affecting (m, nsa) alarm. It is enabled by default.

Action

Step	Action
1	Check the site records to determine the intended configuration data for the affected ring.
2	Open the Configuration Manager tool on the OPC (see *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B).
3	Compare the ring configuration records with the data in the Configuration Manager.

If the Configuration Manager data	Then go to
is correct	step 4
is incorrect	step 7

4	If the Configuration Manager has the correct data, perform a configuration audit according to *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B. *A list of all the network elements with discrepancies in the OPC data appears.*
5	When you are prompted to correct the discrepancies, select the **Yes** option.
6	Go to step 9.

—continued—

Eqp OPC
Configuration audit fail (continued)

Step	Action
7	If the Configuration Manager tool has incorrect data, correct the data in the tool.
8	When the OPC configuration data is correct, select the command **Save and send configuration data**. This command sends the corrected configuration data to the network elements. (For detailed instructions, see *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B).
9	Perform another configuration audit.
10	Use the OPC Alarm Monitor tool to display the active alarms (see *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C). Ensure that the “Configuration audit fail“ alarm has cleared. The alarm clears 1 to 2 minutes after the audit completes successfully. ***Note 1:*** You can also use the OPC Event Browser tool to display the logs for information about the audit. An NAD308 log is present for each audit. ***Note 2:*** For instructions on how to use the Event Browser, see *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C. For more information on the logs, see *Log Report Manual*, 323-3001-840, in *Maintenance*, Volume 5B.
11	If the alarm is still active, repeat this procedure until you have audited all the ring configurations for the OPC span of control and the alarm is no longer active. If the alarm remains active and you are satisfied that the configuration information in the OPC is correct, a data communications problem may exist between the OPC and the affected network elements. Check for data communications alarms and clear them. **—end—**

Eqp OPC
Connection audit fail

Probable cause

A connection audit has detected a discrepancy between the data stored in the Configuration Manager database on the OPC and the data stored on one or more network elements in the OPC span of control. The audit can be either a manual audit (initiated using the OPC Connection Manager tool) or a scheduled audit.

The alarm is raised after a hold-off period of 1 to 2 minutes. It is cleared automatically 1 to 2 minutes after the provisioning conflict has been resolved and a successful connection audit has been performed. You can also manually clear this alarm according to “Manually clearing OPC alarms” on page 1-6. Manually clear the alarm only when the mismatched connection data has been corrected and a configuration audit successfully run.

Impact

This is a minor, not service-affecting (m, nsa) alarm. It is enabled by default.

Action

Step	Action
1	Check the site records to determine the intended connection data.
2	Open the Connection Manager tool on the OPC (see *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B). *A list of all the connections with mismatches between the OPC and network element data appears.*
3	Resolve the mismatches by either editing the connections or deleting them, as appropriate, according to the intended provisioning. (For detailed instructions, see *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B.)

CAUTION
Risk of service interruption
Overwriting the network element data can cause a loss of traffic. Be sure that the network element connection data is inaccurate before overwriting the existing data.

4	Perform a manual connection audit from the OPC using the Connection Manager tool.

—continued—

Eqp OPC
Connection audit fail (continued)

Step	Action
5	Use the OPC Alarm Monitor tool to display the active alarms (see *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C). Ensure that the “Connection audit fail” alarm has cleared. The alarm clears 1 to 2 minutes after the audit completes successfully. ***Note 1:*** You can also use the OPC Event Browser tool to display the logs for information about the audit. An NAD324 log indicates any problems found when manually auditing connection data or when manually correcting mismatched data. ***Note 2:*** For instructions on how to use the Event Browser, see *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C. For more information on the logs, see *Log Report Manual*, 323-3001-840, in *Maintenance*, Volume 5B.
6	If the alarm is still active, repeat this procedure. If you are satisfied that the connection information in the OPC is correct, a data communications problem may exist between the OPC and the affected network elements. Check for data communications alarms and clear them. **—end—**

Eqp OPC
Datasync fail

Probable Cause

A synchronization attempt (database backup) from the primary to the backup OPC has failed. The backup attempt can be either a manual or scheduled operation.

The OPC raises this alarm after a hold-off period of 1 to 2 minutes. The OPC automatically clears this alarm 1 to 2 minutes after it successfully backs up the database. You can also manually clear this alarm according to “Manually clearing OPC alarms” on page 1-6. It is recommended that you manually clear the alarm only when the data synchronization has been successful.

Impact

This is a minor, not service-affecting (m, nsa) alarm. It is enabled by default.

Action

Step	Action
1	Use the OPC Save and Restore tool to attempt to perform a database backup from the primary OPC to the backup OPC (see *Data Administration Procedures*, 323-3001-304, in *Operations, Administration, and Provisioning*, Volume 4A).
2	Use the OPC Alarm Monitor tool to display the active alarms (see *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C). Ensure that the “Datasync Fail” alarm has cleared. The alarm clears 1 to 2 minutes after the audit completes successfully. You can also use the OPC Event Browser tool to display the logs for information about the audit. An SDA622 log indicates that the audit ran successfully on all network elements in the OPC span of control. An SDA322 log indicates that the backup failed and gives the reason it failed. An SDA331 log is displayed for failed backup attempts during network upgrades. For instructions on how to use the Event Browser, see *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C. For more information on the logs, see *Log Report Manual*, 323-3001-840, in *Maintenance*, Volume 5B.
3	If the alarm still exists, repeat steps 1 and 2.
4	If reattempting the operation does not clear the problem, contact your next level of support.

—end—

Eqp OPC
Lost peer OPC

Probable cause

Data communications association has been lost between this OPC and its peer. For example, the fiber between the OPCs has been cut or damaged. If the OPC is the primary OPC, the peer is the backup OPC. If this OPC is the backup OPC, the peer is the primary OPC.

The OPC raises this alarm after a hold-off period of 1 to 2 minutes. The OPC automatically clears this alarm 1 to 2 minutes after communications are reestablished. You can also manually clear this alarm according to "Manually clearing OPC alarms" on page 1-6. It is recommended that you manually clear the alarm only if the root cause of the alarm has been corrected.

Impact

This is a minor, not service-affecting (m, nsa) alarm. It is enabled by default.

The data communications network may be segmented. In this case, the primary OPC controls part of the span of control, and the backup OPC controls the remainder of the span of control. If you make any provisioning changes on the backup OPC in such circumstances, you must also make them on the primary OPC. Otherwise, the changes are lost during the next primary to backup OPC data synchronization.

Action

Step	Action
1	Use the OPC Alarm Monitor tool to display the active alarms (see *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C).
2	Correct the active alarms according to the appropriate procedures in this document.
3	After you clear all other alarms, ensure that the "Lost peer OPC" alarm has cleared. The alarm clears 1 to 2 minutes after the OPCs can again communicate.

—end—

Eqp OPC
NE DB missing/outdated

Probable cause

Either both network element database backups are missing or the most recent one is more than 24 hours old.

The alarm is raised after a hold-off period of 1 to 2 minutes. It is cleared automatically 1 to 2 minutes after all the network element databases are present and up to date. You can also manually clear this alarm according to “Manually clearing OPC alarms” on page 1-6. Manually clear the alarm only if the missing or out of date databases have been successfully backed up to the OPC.

Impact

This is a minor, not service-affecting (m, nsa) alarm. It is enabled by default.

CAUTION
Risk of service interruption
A missing or out of date database can cause the network element to autoprovision during a reboot. This autoprovisioning can result in a loss of service.

Action

Step	Action
1	Use the OPC Backup/Restore Manager tool to check the database backups for each of the network elements. ***Note:*** Each network element is supposed to have two backups, one identified as current and the other as backup1. The date associated with the most recent backup (backup1 if the current backup is missing) should be within 24 hours of the present time.
2	After you identify the missing or out-of-date backup, log in to the affected network element and manually perform a database backup by entering: **equipmnt sh** ↵ **backupdb** ↵ **y** ↵

—continued—

Eqp OPC
NE DB missing/outdated (continued)

Step	Action
3	Verify that the backup was successful by checking for a FWDB400 Database Backup Successful log by entering: **admin nep** ↵ (see Note 1) **logs** ↵ **open fwdb** ↵ **back all** ↵ (see Note 2) ***Note 1:*** If you prefer, instead of entering the **admin nep** and **logs** commands, you can enter the **logutil** command from the command input area or in the command interpreter (CI) level of the user interface. ***Note 2:*** The **back all** command displays all the logs of the requested type currently stored in the logs buffer. Use the **back** command (without the **all** parameter) to display the logs one by one. ***Note 3:*** Refer to the *Log Report Manual*, 323-3001-840, in *Maintenance*, Volume 5B, for a description of the FWDB400 log. Refer to *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C, for a description of how to access logs through the OPC Event Browser tool.
4	Use the OPC Alarm Monitor tool to display the active alarms (see *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C). Ensure that the “NE DB missing/outdated” alarm has cleared. The alarm clears 1 to 2 minutes after all the databases are present and up to date.

—end—

Eqp OPC
OPC alarm(s) active

Probable cause

This is the NE pointer alarm. The OPC raises this alarm at the NE to notify you that one or more OPC alarms are active.

Impact

This is a minor, not service-affecting (m, nsa) alarm. It is inhibited by default.

Action

Correct the problem at the OPC. The OPC automatically clears this alarm.

—end—

Eqp OPC
OPC circuit pack fail

Probable cause

The operations controller (OPC) failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OPC
OPC circuit pack mismatch

Probable cause

The slots provisioned for the OPC do not contain an OPC circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OPC
OPC circuit pack missing

Probable cause

The OPC circuit pack is missing from the shelf, or is improperly seated in the shelf backplane.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

If the OPC module is present, ensure that it is properly seated in the backplane.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If you cannot successfully complete this procedure, contact your next level of support

—end—

Eqp OPC
OPC CNET loss of signal

Probable cause

The OPC can no longer communicate through the control network (CNET).

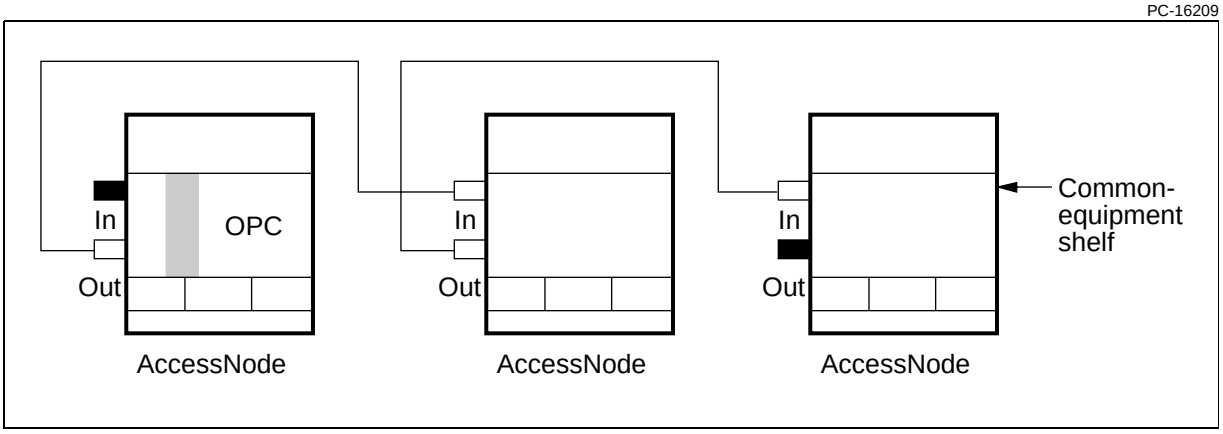
Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Verify the control network cabling at each connection point on each shelf. The following figure shows a block diagram of a typical CNET connection between three common-equipment shelves. The output of one shelf connects to the input of the next shelf. Unused CNET connectors must be terminated with an NT7E5072 termination plug. For ABM shelves: CNET in is J10, and CNET out is J09 on the side interconnect left For TBM shelves: CNET in is J11, and CNET out is J02 on the side interconnect left

PC-16209



	If the CNET cabling is properly connected, replace the OPC as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OPC
OPC Ethernet loss of signal

Probable cause

There is a loss of Ethernet signal between the OPC module and the OPC X-terminal or workstation.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Check that the X-terminal or workstation is powered on.

If the terminal or workstation	Then
is not powered on	turn on the power and check that the alarm has cleared
is powered on	go to step 2

Step	Action
2	Check the X-terminal or workstation modem for proper connection and operation.

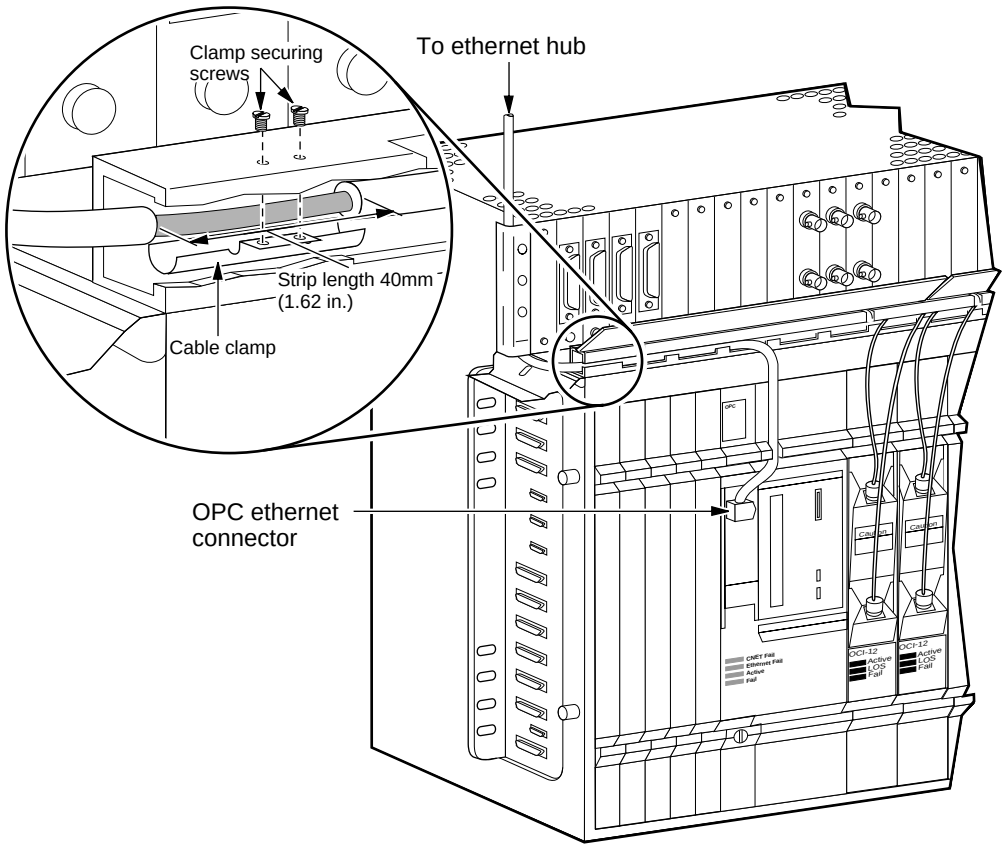
If the modem	Then
is not operational or is not properly connected	correct the problem and check that the alarm clears
is operational	go to step 3

—continued—

Eqp OPC
OPC Ethernet loss of signal (continued)

Step	Action
3	Check the condition of the Ethernet cable and its connections to the OPC module and the X-terminal or workstation. The location of the Ethernet connector on the OPC module is shown in the following figure.

PC-10347



Note: Connection for shelf position 2 shown. Shelf positions 1 and 3 are similar.

If the Ethernet cable is	Then
faulty or improperly connected	correct the fault and verify that the alarm has cleared
not faulty and is properly connected	go to step 4

—continued—

Eqp OPC
OPC Ethernet loss of signal (continued)

Step	Action
4	Verify that the Ethernet ports are properly configured for the OPC and the X-terminal or workstation.

If the Ethernet port is	Then
not configured correctly	correct the configuration and verify that the alarm has cleared.
configured correctly	go to step 5

5	Replace the OPC module as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OPC
OPC hardware reset

Probable cause

The central processing unit in the operations controller (OPC) module has performed a reset.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

This alarm should only be raised once. If the alarm reoccurs, replace the OPC module as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OPC
OPC OAM software fail

Probable cause

This alarm is raised for one of the following reasons:

- data corruption or inconsistencies exist on the OPC hard disk
- the primary OPC is shut down
- a software upgrade is in progress

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

If the alarm is caused by data problems on the OPC hard disk, contact your Nortel Networks service representative and report this alarm.

If the alarm is caused by a shutdown of the primary OPC or a software upgrade, wait to see if the alarm clears on its own once the OPC is back in service or the software upgrade is complete. If not, contact your Nortel Networks service representative and report this alarm.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OPC
OPC serial I/O card mismatch

Probable cause

An incorrect card is in the slot designated for the serial I/O card (NT4K58LA).

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the incorrect card with an NT4K58LA serial I/O card as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OPC
OPC serial I/O card missing

Probable cause

The NT4K58LA serial I/O card is missing.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

If the NT4K58LA serial I/O card is present, ensure that it is properly seated in the slot.

If the NT4K58LA serial I/O card is missing, install a serial I/O card, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp OPC
Tape backup/Restore fail

Probable cause

An attempt to backup to tape, restore a backup from tape, or to display the tape contents has failed. Some problems that can affect tape backup and restore operations are as follows:

- No tape drive exists in the version of the OPC on which the attempt was made.
- No tape is in the tape drive.
- The tape drive is already in use.
- The contents on the tape are unrecognized by the OPC.
- The tape was ejected.
- The tape is write protected.
- The data on the tape is corrupted.
- The data on the tape is not for the correct software release.
- The tape backup between the primary and backup OPCs failed following a restore from tape.
- A software problem exists on the OPC or the disk space on the OPC is full.

The OPC raises the alarm after a period of 1 to 2 minutes. The OPC automatically clears the alarm 1 to 2 minutes after you perform a subsequent backup to tape or restore from tape (depending on which operation failed). You can also manually clear the alarm according to “Manually clearing OPC alarms” on page 1-6. It is recommended that you manually clear the alarm only if a subsequent backup or restore operation has been successfully performed.

Impact

This is a minor, not service-affecting (m, nsa) alarm. It is enabled by default.

—continued—

Eqp OPC
Tape backup/Restore fail (continued)

Action

Step	Action
1	Ensure that the OPC on which you are attempting the operation has a tape drive.
2	Verify that the tape is not damaged and that it contains the backup for the correct OPC and software release. If the OPC detects that the tape is damaged, the message “bad tape” appears when you attempt to perform the backup.

CAUTION
Risk of tape damage
Never store tapes in the sun, near a heat source, or near a magnetic source such as a power converter.

3	If you are backing up to tape, ensure that the tape is not write-protected. You can remove the write protection by closing the tab on the tape. If the write-protection is in place, the message “bad tape” appears when you attempt to perform the backup.
4	Reattempt the data backup or restore operation two more times. After each attempt, use the OPC Alarm Monitor tool to display the active alarms (see *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C). If the message “couldn’t be accessed” appears when you attempt to perform the backup, the failure is most likely the result of a transient condition. If the message “disk full” appears, the OPC disk is full and the backup or restore operation cannot be done until disk space has been made available (go to step 12).
5	If the cause of the problem has been corrected or if the problem was only transient, the “Tape backup/Restore fail” alarm clears 1 to 2 minutes after the operation completes successfully. You can also use the OPC Event Browser tool to display the logs for information about the operation.

—continued—

Eqp OPC
Tape backup/Restore fail (continued)

Step	Action
	For instructions on how to use the Event Browser, see *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C. For more information on the logs, see *Log Report Manual*, 323-3001-840, in *Maintenance*, Volume 5B.
6	The following logs apply: • SDA320 indicates that the backup to tape from the OPC disk has failed (for either a manual or scheduled operation). • SDA321 indicates that the restore from tape to the OPC disk has failed. • SDA322 indicates that the data transfer between the primary and backup OPCs has failed following a data restore from tape operation. • SDA350 indicates a failure in the backup to tape because of a transient error or the OPC disk is full. • SDA351 indicates a failure in the restore from the tape to the OPC disk because of a transient error, the OPC disk is full, or the tape is defective. • SDA620 indicates the completion of a save-to-tape operation. • SDA621 indicates the completion of a restore-from-tape operation. • SDA720 the start of a save-to-tape operation. • SDA721 indicates the start of a restore-from-tape operation.
7	If the same error occurs each time you attempt the operation, remove the tape and reattempt the same procedure with another tape. For a restore operation, use the most recent backup.
8	If the alarm is still active after you use another backup tape, shut down the OPC as described in *Data Administration Procedures*, 323-3001-304, in *Operations, Administration, and Provisioning*, Volume 4A.
9	Reattempt the operation after the OPC reboots.
10	If the alarm remains active, the tape drive might be damaged. Replace the OPC according to *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
11	Check the active alarms using the Alarm Monitor tool. See *OPC User Interface Description*, 323-3001-301, in *Operations, Administration, and Provisioning*, Volume 4A.
12	If the alarm is still active, the original OPC is not at fault. Reinstall the original OPC according to *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
13	Ensure that all other active alarms are cleared, then contact your next level of support. Report the cause of the problem as indicated in any relevant log reports.

—end—

Eqp Proc
Both C-bus access fail

Probable cause

The processor circuit pack has lost communication with the circuit packs on communication bus-A (plane A) and communication bus-B (plane B). This can be due to a faulty processor, TIC, AIC, MIC, TAC, or IRTU.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the processor circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If replacing the processor circuit pack does not clear this alarm, ensure that all AIC, TIC, MIC, TAC and IRTU equipment alarm points are enabled as described in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning,* Volume 4B. (This will prevent potential alarm conditions from being masked.) Check for alarms raised against the following cards, look up the alarms in this document and proceed as instructed:

- transport interface card (TIC) on plane A and plane B
- access interface card (AIC) on plane A and plane B
- maintenance interface card (MIC) on plane A
- test access card (TAC) on plane B
- integrated remote test unit (IRTU) on plane B

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp Proc
C-bus-A access fail

Probable cause

The processor circuit pack has lost communication with the cards on communication bus-A (plane A). This can be due to a faulty processor, TIC, AIC, or MIC on plane A.

Impact

In an unprotected configuration, this is a major, not service-affecting (M, nsa) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the processor circuit pack, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If replacing the processor circuit pack does not clear this alarm, ensure that all AIC, TIC and MIC equipment alarm points are enabled as described in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B. (This will prevent potential alarm conditions from being masked.) Check for alarms raised against the following cards, look up the alarms in this document and proceed as instructed:

- transport interface card (TIC) on plane A
- access interface card (AIC) on plane A
- maintenance interface card (MIC) on plane A

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp Proc
C-bus-B access fail

Probable cause

The processor circuit pack has lost communication with the cards on communication bus-B (plane B). This can be due to an improperly seated I/O card or a faulty processor, TIC, AIC, TAC, or IRTU on plane B.

Impact

In an unprotected configuration, this is a major, not service-affecting (M, nsa) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the processor circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If replacing the processor circuit pack does not clear this alarm, ensure that all AIC, TIC, TAC and IRTU equipment alarm points are enabled as described in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B. (This will prevent potential alarm conditions from being masked.) Check for alarms raised against the following cards, look up the alarms in this document and proceed as instructed:

- transport interface card (TIC) on plane B
- access interface card (AIC) on plane B
- test access card (TAC) on plane B
- integrated remote test unit (IRTU) on plane B

If there are no alarms raised against the above cards, check for an improperly seated I/O card in the I/O portion of the common-equipment shelf.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp Proc
Circuit pack missing

Probable cause

The standby (redundant) processor has been removed from its slot in the common-equipment shelf.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

If the circuit pack is present in the slot, ensure that it is properly seated.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp Proc
Communication processor fail

Probable cause

The processor circuit pack has a failed communications processor.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp Proc
Degraded communication processor

Probable cause

The processor circuit pack has a faulty communications processor.

Impact

In an unprotected configuration, this is a major, not service-affecting (M, nsa) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp Proc
Degraded host processor

Probable cause

The processor circuit pack has a faulty host processor.

Impact

In an unprotected configuration, this is a major, not service-affecting (M, nsa) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp Proc
Degraded master CBIC-A

Probable cause

An improperly seated common-equipment card can cause this alarm, or the processor circuit pack has a faulty master control bus interface chip-A (CBIC-A).

Impact

In an unprotected configuration, this is a major, not service-affecting (M, nsa) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Ensure that all common-equipment circuit packs are properly seated in their respective slots.

If all common-equipment circuit packs are properly seated, replace the processor circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp Proc
Degraded master CBIC-B

Probable cause

An improperly seated common-equipment card can cause this alarm, or the processor circuit pack has a faulty master control bus interface chip-B (CBIC-B).

Impact

In an unprotected configuration, this is a major, not service-affecting (M, nsa) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Ensure that all common-equipment circuit packs are properly seated in their respective slots.

If all common-equipment circuit packs are properly seated, replace the processor circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp Proc
Firmware PROM Fail

Probable cause

The programmable read-only memory (PROM) on the processor circuit pack has failed.

Impact

In an unprotected configuration, this is a Critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp Proc
Interprocessor comm fail

Probable cause

There is no communication between the host processor and the communications processor on the processor circuit pack.

Impact

In an unprotected configuration, this is a major, not service-affecting (M, nsa) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp Proc
Loss of data synchronization

Probable cause

The processor datasync option has been manually changed from datasync on to datasync off.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Set the processor datasync option to datasync on as outlined in the following procedure. If the following procedure does not clear the alarm after four minutes, contact your Nortel Networks service representative.

Step	Action
1	From the network element status screen, display the processor screen: **eq proc <group>**↵ where <group> group number of the processor: **a** or **b** *The processor screen appears.*
2	Enable the datasync option: **datasync on**↵ *The Data Synchronization field will change from off to on. The word "on" appears in reverse video.*
3	Return to the network element status screen: **quit**↵
4	Wait 4 minutes to see if this alarm clears. If it does not clear after 4 minutes, contact your next level of support.

—end—

Eqp Proc
Loss of duplex

Probable cause

The active processor has detected that the standby processor is no longer available as a duplex processor. The standby processor is in either of two states: IS-Trbl or OOS-Mtce.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Although the system is operational, the standby processor is no longer be able to take over processing in the event of a manual or system-initiated switch of activity (SWACT). This condition should be investigated as soon as possible.

Action

Step	Action
1	Ensure that the standby processor is properly inserted and in-service, then check for other higher order alarms against the standby processor. From any screen, display the list of alarms: **alarms**↵ *A list of alarms appears.*

If the processor	Then
has a higher order alarm	look up the alarm in this document and proceed as instructed
does not have a higher order alarm	replace the standby processor as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp Proc
Loss of mate communication

Probable cause

The active processor has lost communication with the standby processor (in a duplex configuration).

Impact

This is a warning, not service-affecting (w, nsa) alarm, raised against the standby processor.

Action

Step	Action
1	Check for other higher order alarms against the standby processor. From any screen, display the list of alarms: **alarms**↵ *A list of alarms appears.*

If the processor	Then
has a higher order alarm	look up the alarm in this document and proceed as instructed
does not have a higher order alarm	replace the standby processor as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp PSU
Circuit pack fail
Circuit pack mismatch
Circuit pack missing

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on the following AccessNode Express power supply unit/ring amplifier alarms and the appropriate alarm clearing procedures.

- Circuit pack fail
- Circuit pack mismatch
- Circuit pack missing

—end—

Eqp SI
Circuit pack fail
Circuit pack mismatch
Circuit pack missing
Signal battery A loss
Signal battery B loss
Talk battery A loss
Talk battery B loss

See the *UE9000 Voice OAM&P User Guide* for information on the following Universal Edge 9000 (UE9000) alarms and the appropriate alarm clearing procedures.

The following alarms are associated with the shelf interface (SI) card on the UE9000 shelf:

- Circuit pack fail
- Circuit pack mismatch
- Circuit pack missing
- Signal battery A loss
- Signal battery B loss
- Talk battery A loss
- Talk battery B loss

—end—

Eqp SPX
Circuit pack fail
Circuit pack mismatch
Circuit pack missing
Duplex SP comms failure
Environmental alarm hw fail
ITU comms failure
ITU datasync fail

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on the following AccessNode Express shelf processor alarms and the appropriate alarm clearing procedures.

- Circuit pack fail
- Circuit pack mismatch
- Circuit pack missing
- Duplex SP comms failure
- Environmental alarm hw fail
- ITU comms failure
- ITU datasync fail

—end—

Eqp SPX
Loss of primary timing reference
Loss of secondary timing reference
SID mismatch
Software release mismatch
SP datasync fail
Timing generation entry to freerun
Upgrade in progress

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on the following AccessNode Express shelf processor alarms and the appropriate alarm clearing procedures.

- Loss of primary timing reference
- Loss of secondary timing reference
- HDT denies connection - unexpected SID (SID mismatch)
- Software release mismatch
- SP datasync fail
- Timing generation entry to freerun
- Upgrade in progress

—end—

Eqp STS1
BNC I/O card 1 fail
BNC I/O card 2 fail
BNC I/O card 3 fail

Probable cause

A component failure or defective circuit pack exists.

Impact

This is a major, service-affecting (M, SA) alarm.

This is a minor, not service-affecting, (m, nsa) alarm.

Action

Step	Action
1	**CAUTION** **Risk of traffic loss** Do not remove BNC input/output (I/O) circuit packs without advice from your Nortel Networks support group. A BNC input/output (I/O) circuit pack has failed and needs replacing. Contact your next level of support. **—end—**

Eqp STS1
BNC I/O card 1 mismatch
BNC I/O card 2 mismatch
BNC I/O card 3 mismatch

Probable cause

The circuit pack inserted into the shelf I/O slot does not match the provisioned circuit pack type.

Impact

This is a major, service-affecting (M, SA) alarm.

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	**CAUTION** **Risk of traffic loss** Do not remove another BNC input/output (I/O) circuit pack, as it will cause the loss of an STS-1 signal. Replace the circuit pack in the I/O slot with a BNC input/output (I/O) circuit pack. ***Note:*** All three interface circuit packs must be inserted even if not all three STS-1 facilities are provisioned.
2	Ensure BNC input/output (I/O) circuit packs are firmly pushed into the backplane of the shelf.

—end—

Eqp STS1
BNC I/O card 1 missing
BNC I/O card 2 missing
BNC I/O card 3 missing

Probable cause

A provisioned shelf I/O slot does not contain a BNC input/output (I/O) circuit pack.

Impact

This is a major, service-affecting (M, SA) alarm.

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Insert a BNC input/output (I/O) circuit pack into the slot. ***Note:*** All three interface circuit packs must be inserted even if not all three STS-1 facilities are provisioned.
2	Ensure BNC input/output (I/O) circuit packs are firmly pushed into the backplane of the shelf.

—end—

Eqp STS1
Circuit pack fail

Probable cause

There is a defective circuit pack.

Impact

This is a critical, service-affecting (C, SA) alarm (if not protectable).

This is a minor, not service-affecting (m, nsa) alarm (if protectable).

Note: Switch to protection initiated, with a maximum 60 ms traffic outage.

Action

Step	Action
1	Replace the defective circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C, for replacement instructions.

—end—

Eqp STS1
Circuit pack mismatch

Probable cause

The circuit pack in the slot does not match the provisioned type.

Impact

This is a critical and service-affecting (C, SA) alarm (if not protectable).

This is a minor, not service-affecting (m, nsa) alarm (if protectable).

Action

Step	Action
1	For an in-service circuit pack, replace the alarmed circuit pack with the proper type. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C, for replacement instructions.

—end—

Eqp STS1
Circuit pack missing

Probable cause

A provisioned slot does not contain a circuit pack.

Impact

This is a critical and service-affecting (C, SA) alarm (if not protectable).

This is a minor, not service-affecting (m, nsa) alarm (if protectable).

Action

Step	Action
1	Insert an STS-1 electrical interface circuit pack into the slot. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C, for replacement instructions.

—end—

Eqp STS1
Firmware failure

Probable cause

A problem exists with the STS-1 electrical interface circuit pack firmware.

Impact

This is a critical and service-affecting (C, SA) alarm (if not protectable).

This is a minor, not service-affecting (m, nsa) alarm (if protectable).

Action

Step	Action

1 Reseat the STS-1 electrical interface circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If	Then
the alarm is raised again	go to step 2
the alarm clears	you have completed the procedure

2 Download firmware to the STS-1 electrical interface circuit pack. See the procedure on verifying the firmware load on an STS-1 electrical interface circuit pack in *Commissioning and Testing,* Volume 3.

If	Then
you cannot download firmware to the circuit pack	go to step 3
the alarm is raised again	go to step 3
the alarm clears	you have completed the procedure

3 Replace the STS-1 electrical interface circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If the alarm	Then
is raised again	go to step 4
clears	you have completed the procedure

4 Contact your next level of support.

—end—

Eqp STS1
Firmware/software incompatible

Probable cause

The firmware on the STS1 circuit pack is older than the baseline required by the software.

Note: This alarm will be raised during software upgrades that require updated firmware. It can also be raised if an STS-1 circuit pack is replaced by another which has firmware not meeting the baseline required by the software.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Do the following:

If	Then
the alarm is raised as part of a software upgrade	no user action is required. Complete the software upgrade procedure. See the procedure on verifying the firmware load of an STS-1 circuit pack in *Commissioning and Testing,* Volume 3.
the alarm is raised but is not part of a software upgrade	download the proper STS-1 firmware release. See the procedure on verifying the firmware load of an STS-1 circuit pack in *Commissioning and Testing,* Volume 3.
you do not know which firmware release is required by your system	see OC-3/OC-12 network element detailed ordering equipment codes in *Engineering and Ordering Information,* 323-3001-032, *Engineering, Configuration, and Ordering Guide,* Volume 1.
you cannot download to the circuit pack	replace the circuit pack. See the procedure for replacing the STS-1 circuit pack in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

2	If you are unable to obtain the necessary information, call your next level of support.

—end—

Eqp STS1
Forced switch request

Probable cause

A forced switch command has been requested for the STS-1 electrical interface circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Note: This alarm point serves as a reminder not to leave a potentially service-affecting condition on the system (especially when conveying live traffic).

No action is required if a test or maintenance operation is being performed.

—end—

Eqp STS1
Lockout request

Probable cause

A lockout command has been issued for the STS-1 electrical interface circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Note: This alarm point serves as a reminder not to leave a potentially service-affecting condition on the system (especially when conveying live traffic).

No action is required if a test or maintenance operation is being performed.

—end—

Eqp STS1
Manual switch request

Probable cause

A manual switch command has been requested for the STS-1 electrical interface circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

No action is required if a test or maintenance operation is being performed.

—end—

Eqp STS1
Protection path fail

Probable cause

The protection switch exerciser failed while attempting to bridge traffic to the protection circuit pack. This indicates that a hardware failure exists on the STS-1 protection path. If an STS-1 working circuit pack requires protection and a failure exists on the protection path, this alarm is raised as a major alarm since traffic is lost. If no protection is required, the unprotected severity is minor.

Impact

This is a major, service-affecting (M, SA) alarm when protection is requested.

This is a minor, not service-affecting (m, nsa) alarm when protection is not requested.

Action

Note 1: Removal of the maintenance interface (MIC) circuit pack causes a loss of access to the user interface ports, and the current user process is stopped. In particular, any UI session is stopped and has to be restarted once the MIC is in place.

Note 2: This alarm can be a result of different circuit packs that make up the protection path. This procedure has the user start by replacing the circuit packs that least affects service. Once the circuit pack that causes the alarm has been found, all previously replaced circuit packs need not be returned to Nortel Networks for repair.

Step	Action
1	Verify the state of the maintenance interface controller (MIC) circuit pack: **eq mic** ↵

If the MIC state is	Then go to
OOS	step 2
IS, IS trbl, or other	step 3

2	Change the operating state of the MIC to IS (in service): **chgstate is** ↵

—continued—

Eqp STS1
Protection path fail (continued)

Step	Action
3	Replace the maintenance interface controller (MIC) circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
4	Run the STS-1 exerciser: **equipmnt sh** ↵ **exercise** ↵

If the alarm is	Then
cleared	you have completed the procedure
not cleared	go to step 5

Step	Action
5	Replace the protection switcher circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
6	Run the STS-1 exerciser: **equipmnt sh** ↵ **exercise** ↵

If the alarm is	Then
cleared	you have completed the procedure
not cleared	go to step 7

Step	Action
7	Replace the STS-1 protection circuit pack equipped in slot 3. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
8	Run the STS-1 exerciser: **equipmnt sh** ↵ **exercise** ↵

If	Then
cleared	you have completed the procedure
not cleared	go to step 9

—continued—

Eqp STS1
Protection path fail (continued)

Step	Action
9	The alarm can be a result of parity errors on the STS-1 links between the transport interface cards and the STS-1 protection circuit pack. To determine if this is the case, use the FLT700 logs. Type the following at the NE UI prompt: **logutil**↵ **open flt**↵ **back**↵ Type **back**↵ until all the logs, which have been generated since the last exerciser run, are viewed.

If the logs	Then
indicate parity errors between the transport slots (slots 9 or 10) and the STS-1 protection circuit pack (slot 3)	go to step 10.
do not indicate parity errors between the transport slots (slots 9 or 10) and the STS-1 protection circuit pack (slot 3)	go to step 12.

10	Replace the transport interface circuit pack indicated in the log. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
11	Run the STS-1 exerciser: **equipmnt sh** ↵ **exercise** ↵

If the alarm is	Then
cleared	you have completed the procedure
not cleared	go to step 12

12	Contact your next level of support.

—end—

Eqp STS1
Protection switch complete

Probable cause

An STS-1 electrical interface circuit pack is switched on the standby unit (caused by a manual, automatic, or forced switch).

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	Determine whether the switch was automatic or manual. **protectn** ↵ **dtlprot sts1** ↵
2	Do the following:

If	Then
a manual operation (manual or forced switch) has been performed	the STS-1 circuit pack is being tested
an automatic switch has been performed	investigate with the STS-1 equipment alarm screen on the network element user interface by entering the following commands

alarms ↵

filter eq ↵

3 If the cause of the switch is still unknown, check whether the facility is out of specification.

facility sts1 <unit> <port #> ↵

where

<unit> is **g1** to **g4** (circuit pack group)

<port#> is **1** to **3**

—end—

Eqp STS1
Protection switch fail

Probable cause

An STS-1 electrical interface circuit pack as a result of an automatic switch, a forced switch or a manual switch, is denied access to the protection bus.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action

1 Is the operating state of the protection circuit pack IS?

equipmnt sts1 p ↵

If	Then
no	step 2
yes	step 3

2 Display the alarm screen and check for other more severe STS1 equipment alarms or MIC equipment alarms.

alarms ↵

If	Then
another STS1 equipment alarm appears	look up the alarm in this chapter and proceed accordingly
a MIC equipment alarm appears	look up the alarm in this chapter and proceed accordingly
no other more severe alarms appear	go to step 3

—continued—

Eqp STS1
Protection switch fail (continued)

Step	Action

3 Verify the state of the maintenance interface controller (MIC) circuit pack:

eq mic ↵

If the MIC state is	Then go to
OOS	step 4
IS trbl or other	step 5
IS	step 6

4 Change the operating state of the MIC to IS (in service):

chgstate is ↵

If	Then
IS trbl or other	step 5
IS	step 6

5 Replace the maintenance interface controller (MIC) circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

6 Replace the protection STS-1 electrical interface circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

—end—

Eqp STS1
STS1 intercard fail

Probable cause

A parity error is detected at the backplane between an STS-1 interface and a transport circuit pack (OC-3/OC-12). The cause of the problem might be at the signal source, signal destination, or on the signal path. This could be due to a hardware fault that exists on the STS-1 interface, the transport circuit pack or the backplane.

Impact

This is a critical, service-affecting (C, SA) alarm if the following conditions are met: the system is in an unprotected configuration and a parity error is detected between an active transport circuit pack and a STS-1 interface.

This is a minor, not service-affecting (m, nsa) alarm if the system is in a protected configuration or a parity error is detected between an inactive transport circuit pack and an STS-1 interface.

Action

Step	Action
1	Display the detailed alarm information for this alarm. See the procedure for displaying a detailed alarm report in *Network Surveillance Procedures*, 323-3001-510, in *Maintenance*, Volume 5C. The signal source and signal destination are indicated by the primary slot and secondary slot number on the detailed alarm screen. *A screen is displayed.*
2	Replace the circuit pack that occupies the primary slot number. See the appropriate procedure in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
3	If the problem persists, replace the circuit pack that occupies the secondary slot number. ***Note:*** If the alarm clears, the circuit pack replaced is the source of the problem. All other circuit packs replaced before this step are functioning properly and need not be returned to NT for repair.
4	If the problem persists, call your next level of support. **—end—**

Eqp STS1
Switcher circuit pack mismatch

Probable cause

The circuit pack inserted into the shelf does not match the provisioned circuit pack type.

Impact

This is a critical, service-affecting (C, SA) alarm (if not protectable).

This is a minor, not service-affecting (m, nsa) alarm (if protectable).

Action

Step	Action
1	Replace the circuit pack in the slot with a protection switcher circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C, for replacement instructions.

—end—

Eqp STS1
Switcher circuit pack missing

Probable cause

The protection switcher circuit pack is missing.

Impact

This is a critical, service-affecting (C, SA) alarm (if not protectable).

This is a minor, not service-affecting (m, nsa) alarm (if protectable).

Action

Step	Action
1	Insert a protection switcher circuit pack in the reserved slot. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C, for replacement instructions.

—end—

Eqp STS1
Traffic problem detected

Probable cause

The protection STS-1 electrical interface circuit pack is not available to provide protection. One of the following conditions exists:

- the protection STS-1 electrical interface circuit pack is already protecting another STS-1 circuit pack group
- the protection STS-1 electrical interface circuit pack is missing
- the protection STS-1 electrical interface circuit pack is faulty
- the protection switcher circuit pack is missing
- the protection group is locked out
- the maintenance interface controller (MIC) circuit pack is missing or out of service

Impact

This is a major, service-affecting (M, SA) alarm (if not protectable).

This is a minor, not service-affecting (m, nsa) alarm (if protectable).

Action

Step	Action
1	Display the STS-1 protection screen. Enter: **pr** ↵ **dtlprot sts1** ↵ *The STS-1 detailed protection screen appears.*

—continued—

Eqp STS1
Traffic problem detected (continued)

Step	Action

2 Check for an active protection event against one of the working STS-1 groups. Do this by looking for an asterisk (*) beside any of the STS-1 groups, under the headings: Forced or AutoSw.

If	Then
a Forced switch is active	release the protection switch
an AutoSwitch is active	fix the problem that caused the switch to occur, then switch back to the working STS-1 circuit pack
there are no active protection switches	go to step 3

3 From the same screen as in step 2, check for a lockout against the protection STS-1 circuit pack. Do this by looking for an asterisk (*) beside the P (protection) group, under the Lockout column.

If the protection mapper	Then
is locked out	release the lockout
is not locked out	go to step 4

4 From the same screen as in step 2, check for a lockout against the failed STS-1 circuit pack. Do this by looking for an asterisk (*) beside the failed mapper's circuit pack group, under the Lockout column.

If the failed mapper	Then
is locked out	release the lockout
is not locked out	go to step 5

5 Ensure that the protection STS-1 electrical interface circuit pack is properly installed in shelf slot 3, and that the Active LED is lit.

At this stage, protection is now available and this alarm should clear. Other alarms should be raised, for instance, STS1 circuit pack fail.

If this is	Then
not the case	go to step 6
the case	clear the new alarms

—continued—

Eqp STS1
Traffic problem detected (continued)

Step	Action

6 Ensure that the protection STS-1 electrical interface circuit pack is provisioned and is in service.

If this is	Then
not the case	place the circuit pack in service
the case	go to step 7

7 Ensure that the protection switcher circuit pack is properly installed in shelf slot 2.

If this is	Then
not the case	correct the situation
the case	go to step 8

8 Ensure that the MIC is properly installed, is in service, and that the Active LED is lit.

If this is	Then
not the case	correct the situation
the case	go to step 9

9 Replace the protection STS-1 electrical interface circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.

If the alarm	Then
does not clear	go to step 10
clears	you have completed the procedure

10 Contact your next level of support.

—end—

Eqp STS1
VT connection provisioning mismatch

Probable Cause

One of the following conditions exists:

- a VT1.5 add-drop connection of the STS-1 is provisioned with the VT group and VT number mismatched with the transport STS VT group and VT number
- A VT1.5 add-drop connection with another DS1/STS-1/OC-3 port is provisioned using the transport STS channel that is allocated for VT1.5 connections of the STS-1 port and vice versa
- A VT1.5 passthrough connection is provisioned using the transport STS channel that is allocated for VT1.5 connections of the STS-12 port and vice versa

Impact

This is a minor, not service-affecting (m, nsa) alarm (if protectable).

Action

Step	Action
1	Delete the mismatched VT1.5 connection. See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B.

—end—

Eqp TAC
Circuit pack fail

Probable cause

The test access card (TAC) failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TAC
Circuit pack mismatch

Probable cause

The circuit pack in the slot designated for the test access card does not match the provisioned circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TAC
Circuit pack missing

Probable cause

The test access card is missing from its designated slot.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

If the circuit pack is present in the slot, ensure that it is properly seated.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TAC
Digital side fail

Probable cause

The digital side of the test access card failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you want to obtain additional information about the failure, display the TAC equipment screen, take the TAC out of service, and perform a diagnostic. The diagnostic failure results are reported in log report EQP322.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TAC
Metallic side fail

Probable cause

The metallic side of the test access card failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you want to obtain additional information about the failure, display the TAC equipment screen, take the TAC out of service, and perform a diagnostic. The diagnostic failure results are reported in log report EQP322.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TAC
PGTC I/O card mismatch

Probable cause

The card in the slot designated for the PGTC/MTA input/output card does not match the provisioned circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TAC
Software download fail

Probable cause

The software load for the test access card does not exist on the operations controller (OPC), or the TAC load file transfer from the OPC failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Use the lomui command to verify that the TAC software load exists. At the OPC prompt, type: **lomui query_loads** *A list of all the loads installed on the NE appears.*
2	Does the TAC software load exist?

If the TAC software load	**Then**
exists	go to step 3
does not exist	contact your next level of support

Step	Action
3	If the TAC software load already exists, reload the TAC software, as outlined in the Reboot/Load Manager software procedures in *Commissioning and Testing*, Volume 3.

If the alarm	**Then**
clears	end the procedure here
persists	go to step 4

—continued—

Eqp TAC
Software download fail (continued)

Step	Action
4	If the TAC still fails to load, open the event browser tool and check for the possible reason why the software does not load. If you do not know how to do this, see the procedures for logging in to the OPC and opening an OPC tool in *OPC User Interface Description,* 323-3001-301, in *Operations, Administration and Provisioning,* Volume 4A. If you cannot continue after you check the event browser, contact the system administrator to ensure the load is present, is not corrupted, and has been properly installed. (If the load is not present, it must be copied from tape.)
5	For additional information check the TAC logs for the TAC301 “Restart Fail” log.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TAC
TAP I/O card mismatch

Probable cause

The card in the slot designated for the test access path (TAP) input/output card does not match the provisioned circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TAC
TBP I/O card mismatch

Probable cause

The card in the slot designated for the test bypass pair (TBP) input/output card does not match the provisioned circuit pack.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TDM
A-link clock driver fail
Circuit pack fail
Circuit pack mismatch
Circuit pack missing
Control link fail to TDM-A
Control link fail to TDM-B

See the *UE9000 Voice OAM&P User Guide* for information on the following Universal Edge 9000 (UE9000) alarms and the appropriate alarm clearing procedures.

The following alarms are associated with the time division multiplexor (TDM) card on the UE9000 shelf:

- A-link clock driver fail
- Circuit pack fail
- Circuit pack mismatch
- Circuit pack missing
- Control link fail to TDM-A
- Control link fail to TDM-B

—end—

Eqp TDM
D-link interface fail
Loss of mate communication
PCM path fail to TDM-A
PCM path fail to TDM-B
TDM inter-plane fail

See the *UE9000 Voice OAM&P User Guide* for information on the following Universal Edge 9000 (UE9000) alarms and the appropriate alarm clearing procedures.

The following alarms are associated with the time division multiplexor (TDM) card on the UE9000 shelf:

- D-link interface fail
- Loss of mate communication
- PCM path fail to TDM-A
- PCM path fail to TDM-B
- TDM inter-plane fail

—end—

Eqp TIC
Backplane parity error

Probable cause

The transport interface card failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TIC
Circuit pack fail

Probable cause

The transport interface card failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TIC
Circuit pack mismatch

Probable cause

The circuit pack in the slot designated for the transport interface card does not match the provisioned circuit pack. This alarm can also be caused by a TIC with an incorrect vintage.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the mismatched circuit pack with a circuit pack bearing the correct product equipment code, and correct vintage, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TIC
Circuit pack missing

Probable cause

The transport interface card is missing from its designated slot.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

If the circuit pack is present in the slot, ensure that it is properly seated.

If the slot is empty, install a circuit pack bearing the correct product equipment code.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TIC
Loss of signal synchronization

Probable cause

Signalling between the two TICs is lost.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Replace the secondary TIC, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end the procedure
persists	go to step 2

Step	Action
2	Replace the primary TIC, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end the procedure
persists	if you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TIC
T-link interface fail

Probable cause

The system has detected a failure on the T-link between the transport interface card (TIC) and the access interface card (AIC).

Note: This same alarm is also raised as an equipment alarm against the corresponding AIC.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

If the severity of this alarm is warning, not service-affecting (w, nsa), the problem is most likely associated with the card at the other end of the link.

Action

Step	Action

If the severity of this alarm is	Then
C, SA	go to step 1
m, nsa	go to step 1
w, nsa	go to step 2

1 Replace the TIC against which this alarm is raised, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If this alarm	Then
clears	end the procedure
persists	go to step 2

2 From any FWPUI screen, display the list of active alarms:

alarms.↵

The list of active alarms appears.

—continued—

Eqp TIC
T-link interface fail (continued)

Step	Action

3 Identify from the list of active alarms, the **T-link interface fail** alarm raised against the AIC, and display the detailed alarm report:

dtlalms < alarm # >↵

where

< alarm # >	the alarm report number displayed on screen

The detailed alarm screen appears, showing the shelf and slot number of the card.

4 Replace the card identified in the previous step, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If the alarm	Then
persists	go to step 5
clears	end the procedure

5 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TIC
TR-08 circuit pack mismatch

Probable cause

The model of transport interface card (TIC) does not support TR-08 service.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the TIC that raised this alarm with model NT4K56AC or NT4K56CA or later, as described in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

Note 1: Both TICs (primary and secondary) should be the same model (either NT4K56AC or NT4K56CA).

Note 2: The NT4K56AC supports TR-08 signaling on STS-1 #1; NT4K56CA supports TR-08 signaling on STS-1 #1, #2, and #3.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Circuit pack failure

Probable cause

The timing and cross-connect (TXC) card failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Replace the circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Circuit pack mismatch

Probable cause

The circuit pack in the slot designated for the timing and cross-connect (TXC) card does not match the provisioned circuit pack or the TXC circuit pack that raised the alarm has a defective ID PROM.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	If a TXC card is not currently in the slot, replace the mismatched circuit pack with a circuit pack bearing the correct product engineering code, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
2	If there is a TXC card in the slot, then the ID PROM is faulty. In an unprotected configuration, no immediate action is required. Schedule a card replacement of the TXC card during a low traffic period if the card is carrying traffic. In a protected configuration, replace the card as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.
3	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Circuit pack missing

Probable cause

The provisioned timing and cross-connect (TXC) card is missing.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	In the empty slot, install a circuit pack bearing the correct product equipment code, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.
2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
End VCO range

Probable cause

The Stratum-3, voltage controlled oscillator (VCO) on the timing and cross-connect (TXC) card has exceeded 2/3 of its adjustment range.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

The clock may be unable to track changes to the external timing reference.

Action

Step	Action
1	Display the protection switching screen: **pr** ↵ *The NE Transport Protection screen appears.*
2	Display the timing reference protection screen: **trefprot** ↵ *The reference protection screen appears.*
3	Operate the manual switch: **manual op < timing reference >** ↵ **y** ↵ where <timing reference> primary or secondary timing reference: **pri** or **sec**

If the alarm	Then
clears	Check the timing reference input to the TXC card. If the input is bad, fix the timing reference input. If the input is not bad, replace the TXC card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. End the procedure.
persists	go to step 4

4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Equipment lockout request

Probable cause

A lockout request was made for the timing and cross-connect (TXC) cards.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

TXC protection switching is unavailable while the lockout is in effect. TXC card G1 (slot 9) is made the active TXC card. If the lockout request is not cleared, the protection unit TXC G2 (slot 10) is not available for use by the system in the event of a problem with the TXC G1 (slot 9).

This alarm remains in effect until the lockout is cleared.

Action

No action is required unless you want to release the lockout request.

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr**↵ *The protection switching screen appears.*
2	Display the detailed protection screen: **dtlprot txc**↵ *The detailed protection screen appears.*
3	Release the forced switch:
4	**forced re < group >**↵ **y**↵ where < group > group number of the TXC: **g1** or **g2**
5	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Eqp TXC
Equipment protection switch complete

Probable cause

A switch from the working timing and cross-connect (TXC) card to the protection TXC card was successfully completed.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

If the completed protection switch alarm is the result of a manual protection request, this alarm clears automatically. If this alarm is the result of a lockout or forced protection switch request, this alarms remains raised until the lockout or forced request is released.

If the completed protection switch alarm is the result of an automatic protection request, then there may be a fault on the inactive TXC card.

Action

Step	Action
1	Display a list of active alarms for the network element: **alarms.**↵ ***Note:*** In the case of a point-to-point configuration with an FCOT and RFT, display the active alarms at both the local and remote network element.
2	Check for Eqp TXC `Manual equipment lockout request` and Eqp TXC `Forced equipment switch request` alarms.

If either of these alarms is	Then
in effect	look up the alarm in this chapter and proceed accordingly
not in effect	go to step 3

3	If the protection switch is the result of an automatic protection request, check for other TXC alarms and use the procedures in this document to clear the alarms.
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Equipment protection switch fail

Probable cause

A timing and cross-connect (TXC) protection switch has failed because one or both of the TXC cards is faulty or is missing from the shelf.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

The alarm clears when a TXC protection switch completes successfully.

Action

Step	Action
1	Check that there are no lockouts in effect: **eq txc;dtlprot.**↵ *The TXC protection screen appears.*
2	Is there an asterisk (*) in the Lockout column?

If	Then
no	go to step 3
yes	go to step 5

3 Is each operating state IS Normal?

If	Then
no	go to step 4
yes	go to step 7

—continued—

Eqp TXC
Equipment protection switch fail (continued)

Step	Action

4 Display the alarm screen and check for other more severe TXC equipment alarms.

alarms↵

If	Then
another TXC equipment alarm appears	look up the alarm in this chapter and proceed accordingly
no other more severe alarms appear	go to step 7

5 Release the lockout:

lockout re ↵
y↵

The screen displays a period (.) in the `Lockout` *column for the corresponding group.*

6 Perform a forced protection switch to the standby TXC card:

forced op < group >↵
y↵

where

< group >	group number of the TXC that is currently active: **g1** or **g2**

If the protection switch	Then
succeeds	end the procedure
fails	go to step 4

7 Replace the standby TXC card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

8 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Equipment prot oscillation control activated

Probable cause

The system has automatically disabled TXC protection switching because more than five firmware initiated protection switches were detected within 1 minute.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

TXC card G1 (in slot 9) is made the active TXC card and TXC protection is not available

Action

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr**↵ *The protection switching screen appears.*
2	Display the detailed protection screen: **dtlprot txc**↵
3	*The detailed protection screen appears.*
4	Release the TXC lockout: **lockout re**↵ **y**↵
5	Observe the detailed protection screen for 5 minutes. If the equipment is still switching automatically, proceed to replace the TXC card that is inactive most of the time. For details, refer to *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Failure to lock

Probable cause

The timing and cross-connect (TXC) circuit packs have exceeded the threshold time allowed for locking to (acquiring) the input timing reference signal.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Verify the integrity of the input timing reference signal and correct any problems.
2	Attempt to acquire the signal again as follows:

a. Display the TXC Reference Protection screen:

pr;trefprot↵

The TXC Reference Protection screen appears.

b. Operate a manual timing reference protection switch to the failed reference:

manual op < timing reference >↵

where

< timing reference >	primary or secondary timing reference (whichever is currently active): **pri** or **sec**

The screen displays an asterisk (*) under the heading Manual.

If the alarm	Then
clears	end the procedure
persists	go to step 3

—continued—

Eqp TXC
Failure to lock (continued)

Step	Action
3	Verify that the DS1 facility from which the TXC is sourced is operational and is provisioned correctly as follows: **a.** From the Network Element Status screen, display the DS1 facility provisioning screen: **fa ds1 < group > < port >; edit**↵ where < group > DS1 group number:**g1**, **g2** or **g4** < port > number of the DS1 port: **1** to **14,** or **all** *The DS1 facility provisioning screen appears.* **b.** Check the DS1 facility parameters and correct any incorrect values. ***Note:*** For details see the procedure for provisioning DS1 facility parameters in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B.

If the alarm	Then
clears	end the procedure
persists	go to step 4

4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Forced equipment switch request

Probable cause

A forced protection switch was requested for the timing and cross-connect (TXC) cards.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

The alarm clears when the forced switch request is cleared. If the forced switch request is not cleared, the protection unit is not available for use by the system in the event of a problem with the working TXC.

Action

Step	Action
1	From the Network Element Status screen, display the protection switching screen: **pr**↵ *The protection switching screen appears.*
2	Display the TXC detailed protection screen: **dtlprot txc**↵ *The detailed protection screen appears.*
3	Release the forced switch:
4	**forced re < group >**↵ **y**↵ where < group > group number of the TXC: **g1** or **g2**
5	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Eqp TXC
Forced timing reference switch request

Probable cause

A forced timing reference protection switch was requested for the TXC synchronization references.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

The alarm clears when the forced timing reference switch request is cleared. If the forced request is not cleared, the protection timing reference is not available for use by the system in the event of a problem with the selected timing reference.

Action

Step	Action
1	Display the timing reference protection screen: **pr;trefprot** ↵ *The reference protection screen appears:*
2	Release the forced switch: **forced re < timing reference >** ↵ where <timing reference> primary or secondary timing reference: **pri** or **sec** *A request for confirmation of the action appears.*
3	Confirm the request: **y** ↵
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Intercard: STS1 parity error or clock fail

Probable cause

A failure has occurred between the TXC card and another circuit pack. Not enough information exists to fail either card, so an intercard alarm is raised.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Display the detailed alarm information for this alarm. *The Detailed Alarm Report screen appears.*
2	From the Detailed Alarm Reports screen, record the slot numbers of the primary and secondary circuit packs. ***Note:*** The primary and secondary slot numbers refer to circuit packs on the common-equipment shelf. The PEC for the primary and secondary circuit packs may not be shown on the screen.
3	Determine which cards occupy the primary and secondary slots and record this information.

—continued—

Eqp TXC
Intercard: STS1 parity error or clock fail (continued)

Step	Action
4	Determine the status (active or inactive) of the cards that occupy the primary and secondary slots. ***Note:*** Access the appropriate equipment screen to determine the whether the card is active or inactive.

If	Then
either the primary or secondary card is inactive	a. Replace the inactive card as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C. b. If the alarm clears, end the procedure. c. If the alarm persists, replace the other card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. d. Go to step 5.
both cards are active	a. Replace the card in the primary slot numbers as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. b. If the alarm clears, end the procedure. c. If the alarm persists, replace the other card in the secondary slot as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. d. Go to step 5.

5	Reinsert any card that you replaced in step 3 that did not result in this alarm being cleared. For details, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Manual equipment switch request

Probable cause

A manual protection switch was requested for the timing and cross-connect (TXC) cards.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

This alarm clears automatically when the manual protection switch completes. No action is required.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Manual timing reference switch request

Probable cause

A manual timing reference protection switch was requested for the synchronization references.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

This alarm clears automatically. No action is required.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Partial circuit pack fail

Probable cause

The timing and cross-connect (TXC) circuit pack timing related circuitry failed.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Replace the failed TXC circuit pack as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.
2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Serial link failure

Probable cause

Communication with the mate timing and cross-connect (TXC) card across the inter-card serial link has failed. The alarm is raised by the TXC card that detects the failure.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action

1 Replace the inactive TXC card as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If the alarm	Then
clears	end the procedure
persists	go to step 2

2 From the Network Element Status screen, display the protection switching screen:

pr↵

The protection switching screen appears.

3 Display the detailed protection screen:

dtlprot txc↵

The detailed protection screen appears.

4 Operate the forced switch to the inactive TXC card:

5 **forced op < group >**↵
y↵

where

< group >	group number of the active TXC: **g1** or **g2**

6 Replace the mate TXC card (currently inactive) as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

7 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Sys clock src entry to freerun

Probable cause

This alarm is caused by any of the following conditions:

- the TXC card has just auto provisioned and the clock has not yet been provisioned with a value of DS1linetimed.
- the system clock has been manually set to freerun
- the system clock has entered freerun due to a failure of the timing reference circuitry on an unprotected TXC card

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	From the Network Element Status screen, display the equipment screen for the network element: **eq sh.**↵ *The Shelf Equipment screen appears.*
2	Check the clock source for the shelf.

If the system clock	Then
has just auto provisioned or has inadvertently been provisioned to freerun	go to step 3
is set to ds1linetimed	go to step 4

—continued—

Eqp TXC
Sys clock src entry to freerun (continued)

Step	Action
3	Provision the clock source for the shelf: **edit;clocksrc ds1linetimed↵** **yes↵**

If the alarm	Then
clears	end the procedure
persists	go to step 4

4	Check for a TXC Partial circuit pack fail alarm and use the appropriate procedure in this document to clear the alarm.
5	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Timing gen entry to acquire mode

Probable cause

The timing and cross-connect (TXC) card is in acquisition (acquire) mode. The TXC is in the process of locking to the input timing reference signal. The acquire mode is typically present on power-up or system reset, until synchronization is achieved.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

No action is required. This alarm clears automatically.

A “Timing reference lock failure” alarm is raised if the TXC remains in the acquire mode as a result of failing to track its reference within 2 minutes.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Timing gen entry to fast mode

Probable cause

The timing and cross-connect (TXC) card is in fast acquisition (fast) mode. The TXC timing circuitry has acquired the input timing reference signal and is attempting to lock to it.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

No action is required. This alarm clears automatically when the TXC frequency is adjusted to the reference input frequency.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Timing gen entry to freerun mode

Probable cause

The timing and cross-connect (TXC) has dropped into freerun mode (running off its own clock) because

- the target filter mode has been manually set to freerun
- the 51 Mhz reference clock on the TXC card is unable to lock to an external timing reference (and the timing reference is not protected)
- the selected timing input reference has failed and a protection switch to a good reference is not possible

Impact

This is a warning, not service-affecting (w, nsa) alarm.

The TXC card is in freerun mode (running off its own clock). The voltage controlled oscillator (VCO) is set at the midpoint and is providing a stratum 3 clock.

Action

Step	Action
1	Determine if the TXC target filter mode was is inadvertently set to freerun mode.

If the target filter mode was	Then
inadvertently set to freerun	go to step 2
was not inadvertently set to freerun	go to step 3

—continued—

Eqp TXC
Timing gen entry to freerun mode (continued)

Step	Action
2	From the TXC equipment screen, provision the target filter mode for the TXC clock: **eq txc <group>;edittarg normal**↵ where <group> TXC group number: **g1** or **g2**

If the alarm	Then
clears	end the procedure
persists	go to step 3

3	Display the protection switching screen: **pr** ↵ *The NE Transport Protection screen appears.*
4	Display the timing reference protection screen: **trefprot** ↵ *The reference protection screen appears.*
5	Determine if a forced protection switch or lockout is in effect. ***Note:*** *The screen displays an asterisk (*) under the heading* `Lockout` *or* `Forced` *if either of these commands are in effect.*

If either is	Then
in effect	go to step 6
not in effect	go to step 9

6	Release the lockout or forced switch: **< command > re < timing reference >**↵ where < command > is the protections switch command: **lockout** or **forced** <timing reference> primary or secondary timing reference: **pri** or **sec** *A request for confirmation of the action appears:*
7	Confirm the request: **y** ↵

—continued—

Eqp TXC
Timing gen entry to freerun mode (continued)

Step	Action
8	Determine if the alarm clears.

If the alarm	Then
clears	end the procedure
persists	go to step 9

Step	Action
9	Check for timing reference input failure alarms: **alarms**↵

If the input is	Then
not failed	replace the TXC card that raised the alarm, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C
failed	use the appropriate procedures in this manual to clear the alarms

Step	Action
10	If the selected timing reference input is not failed, replace the TXC card that raised the alarm, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C.
11	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Timing gen entry to holdover mode

Probable cause

The timing and cross-connect (TXC) card is in holdover mode due to a manual request.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Holdover means the TXC card maintains its synchronization based on the last good reference signal.

Action

Step	Action

1 Determine if the TXC target filter mode was inadvertently set to holdover mode.

If the target filter mode was	Then
inadvertently set to holdover	go to step 2
was not inadvertently set to holdover mode	go to step 3

2 From the TXC equipment screen, provision the target filter mode for the TXC clock:

eq txc <group>;edittarg <mode>↵

where

<group>	TXC group number: **g1** or **g2**
<mode>	is the target filter mode of the TXC clock: **normal**, **freerun**

Note: A failure of the active timing reference when a lockout or forced switch is in effect will generate an Eqp TXC `Timing gen entry to freerun mode` alarm.

3 If both the timing references fail but a recovery occurs, this alarm clears when the TXC enters fast mode or acquire mode.

4 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Timing generation primary reference fail

Probable cause

The provisioned primary timing reference input signal is not being detected by either of the timing and cross-connect (TXC) cards.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Access the TXC Timing Reference source screen: **eq txc < group >;trefprot;trefsrc**↵ where <group> TXC group number: **g1** or **g2** *The NE Timing Reference screen appears.*
2	Verify that the primary timing reference is correctly assigned to the appropriate DS1 facility and record the group number and port of the primary timing reference.

If the primary timing reference is	Then
correct	go to step 3
not correct	correct the assignment. For details, see the procedure for provisioning timing and cross-connect parameters in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B. End the procedure.

—continued—

Eqp TCX
Timing generation primary reference fail (continued)

Step	Action
3	Access the DS1 facility screen for the DS1 that is assigned as the primary timing reference: **fa ds1 < group > < port >; edit↵** where < group > DS1 group number recorded in step 2 < port > number of the DS1 port recorded in step 2
4	Check that the DS1 facility is `IS-Normal`.

If the DS1 is	Then
IS-Normal	go to step 5
not IS-Normal	check for DS1 facility alarms and use the appropriate procedures in this manual to clear the alarms.

5	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Timing generation secondary reference fail

Probable cause

The provisioned secondary timing reference input signal is not being detected by either of the timing and cross-connect (TXC) cards.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Access the TXC Timing Reference source screen: **eq txc < group >;trefprot;trefsrc**↵ where <group> TXC group number: **g1** or **g2** *The NE Timing Reference screen appears.*
2	Verify that the secondary timing reference is correctly assigned to the appropriate DS1 facility and record the group number and port of the secondary timing reference.

If the secondary timing reference is	Then
correct	go to step 3
not correct	correct the assignment. For details, see the procedure for provisioning timing and cross-connect parameters in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration and Provisioning*, Volume 4B. End the procedure.

—continued—

Eqp TXC
Timing generation secondary reference fail (continued)

Step	Action
3	Access the DS1 facility screen for the DS1 that is assigned as the secondary timing reference: **fa ds1 < group > < port >; edit↵** where < group > DS1 group number recorded in step 2 < port > number of the DS1 port recorded in step 2
4	Check that the DS1 facility is `IS-Normal`.

If the DS1 is	Then
IS-Normal	go to step 5
not IS-Normal	check for DS1 facility alarms and use the appropriate procedures in this manual to clear the alarms.

5	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Timing ref lockout request

Probable cause

A manual timing reference lockout request was made for the timing and cross-connect (TXC) synchronization references.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Timing reference protection switching is unavailable while the lockout is in effect. If the lockout request is not cleared, the protection timing reference is not available for use by the system if a problem occurs with the working timing reference.

This alarm remains in effect until the lockout is cleared.

Action

No action is required unless you want to release the lockout request.

Step	Action
1	Display the protection switching screen by entering: **pr** ↵ *The NE Transport Protection screen appears.*
2	Display the timing reference protection screen by entering: **trefprot** ↵ *The reference protection screen appears.*
3	Release the lockout by entering: **lockout re < timing reference >** ↵ where <timing reference> primary or secondary timing reference: **pri** or **sec** *A request for confirmation of the action appears.*
4	Confirm the request by entering: **y** ↵
5	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Timing ref prot oscillation control activated

Probable cause

An automatic timing reference lockout has been requested.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Replace both timing and cross-connect (TXC) cards. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If the alarm	Then
clears	end the procedure
persists	contact your next level of support

—end—

Eqp TXC
Timing ref prot switch complete

Probable cause

Synchronization timing was successfully switched from one timing reference to another.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

This alarm clears automatically. No action is required.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Eqp TXC
Timing ref prot switch fail

Probable cause

A synchronization timing reference switch failed.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action

1 If the request for the timing reference protection switch was a manual request, release the request, then try it again. For directions, see *Protection Switching Procedures*, 323-3001-311, in *Operations, Administration, and Provisioning*, Volume 4B.

If the alarm	Then
clears	end the procedure
does not clear	go to step 2

2 Perform a manual protection switch on the timing and cross-connect (TXC). For directions, see *Protection Switching Procedures*, 323-3001-311, in *Operations, Administration, and Provisioning*, Volume 4B.

If the alarm	Then
clears	go to step 3
does not clear	contact your next level of support

3 Replace the inactive TXC. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

4 Perform a manual protection switch on the TXC. For directions, see *Protection Switching Procedures*, 323-3001-311, in *Operations, Administration, and Provisioning*, Volume 4B.

If the alarm	Then
clears	end the procedure
does not clear	contact your next level of support

—end—

Eqp UE
TDM firmware mismatch
Upgrade in progress

See the *UE9000 Voice OAM&P User Guide* for information on the following Universal Edge 9000 (UE9000) alarms and the appropriate alarm clearing procedures.

The following alarms are associated with the UE9000 shelf:

- TDM firmware mismatch
- Upgrade in progress

—end—

Clearing a facility alarm

This chapter describes how to clear facility-class (Fac) alarms. The alarms in this chapter appear alphabetically within alarm types (for example, COMM, DS1, or TIC). The banner at the beginning of each alarm shows the alarm type and the text of the alarm. The procedure describes the cause of the alarm and the action needed to clear it.

Chapter contents

The following tables organize facility (Fac) alarms by alarm type. Each table lists the alarms within a type and the page numbers for the alarm procedures.

> ***Note:*** If you cannot find an alarm in this book, see *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543 for ANX voice module alarms.

Table 4-1
Fac COMM alarms

Alarm	See
Faulty path	page 4-10
No active path	page 4-12
OMC link fail	page 4-13
OMC performance degraded	page 4-16
SONET DCC link fail	page 4-19
SONET DCC performance degraded	page 4-21

Table 4-2
Fac DS1 alarms

Alarm	See
CSU line loopback	page 4-22
Facility loopback	page 4-22
High traffic threshold exceeded	page 4-23
Line Rx CV threshold 1, 2, Line Rx ES threshold 1, 2, Line Rx SES threshold 1, 2	page 4-24
Loopback	page 4-27
Low traffic threshold exceeded	page 4-28
Network loopback	page 4-22
Path Rx CV threshold 1, 2, Path Rx ES threshold 1, 2, Path Rx SAS threshold 1, 2, Path Rx SES threshold 1, 2, Path Rx UAS threshold 1, 2	page 4-29
PRI link OOS	page 4-32
Rx AIS	page 4-33
Rx babbling	page 4-34
Rx bipolar violation > 10E-3	page 4-35
Rx bipolar violation > 10E-4	page 4-38
Rx loss of frame	page 4-39
Rx loss of signal	page 4-42
Rx yellow	page 4-44
STS1 path CV threshold 1, 2 STS1 path ES threshold 1, 2 STS1 path SES threshold 1, 2 STS1 path UAS threshold 1, 2	page 4-45
STS1 Rx path trace failure	page 4-50
STS1 Rx RFI	page 4-53
STS1 Rx unequipped	page 4-55
STS1 signal label mismatch	page 4-57
—continued—	

Table 4-2 (continued)
Fac DS1 alarms

Alarm	See
Terminal loopback	page 4-22
VT Rx AIS	page 4-58
VT Rx loss of pointer	page 4-60
VT Rx RFI	page 4-64
VT Rx unequipped	page 4-66
—end—	

Table 4-3
Fac DS3 alarms

Alarm	See
Frequency out of range	page 4-68
Line FE CV threshold 1, 2, Line FE ES threshold 1, 2, Line FE SES threshold 1, 2, Line FE UAS threshold 1, 2	page 4-70
Line Rx CV threshold 1, 2, Line Rx ES threshold 1, 2, Line Rx SES threshold 1, 2	page 4-71
Loopback	page 4-73
Parity error rate >10E-6	page 4-74
Path Rx AISS threshold 1, 2, Path Rx CV threshold 1, 2, Path Rx ES threshold 1, 2, Path Rx SES threshold 1, 2, Path Rx SEFS threshold 1, 2, Path Rx UAS threshold 1, 2	page 4-75
Path Tx AISS threshold 1, 2, Path Tx CV threshold 1, 2, Path Tx ES threshold 1, 2, Path Tx SES threshold 1, 2, Path Tx SEFS threshold 1, 2, Path Tx UAS threshold 1, 2	page 4-79
Rx AIS	page 4-82
Rx bipolar violation > 10E-3	page 4-83
Rx loss of frame	page 4-85
Rx loss of signal	page 4-87
STS1 path FE CV threshold 1, 2 STS1 path FE ES threshold 1, 2 STS1 path FE SES threshold 1, 2 STS1 path FE UAS threshold 1, 2	page 4-89
STS1 Rx path trace failure	page 4-90
STS1 Rx RFI	page 4-93
STS1 Rx unequipped	page 4-94
STS1 signal label mismatch	page 4-96
—continued—	

Table 4-3 (continued)
Fac DS3 alarms

Alarm	See
Tx AIS	page 4-97
Tx loss of frame	page 4-98
—end—	

Table 4-4
Fac DSX1 alarms

Alarm	See
Facility loopback	page 4-100
Rx AIS	page 4-100
Rx babbling	page 4-100
Rx bipolar violation > 10E-3	page 4-100
Rx bipolar violation > 10E-4	page 4-100
Rx loss of frame	page 4-100
Rx loss of signal	page 4-100
Rx yellow	page 4-100
Terminal loopback	page 4-100

Table 4-5
Fac ESI alarms

Alarm	See
Bipolar violation	page 4-101
Degraded clock carrier	page 4-102
Degraded timing reference	page 4-103
Loss of frame	page 4-104
Loss of signal	page 4-106
Oscillating sync status message	page 4-108
Reference forced switch request	page 4-109
Reference manual switch request	page 4-110
Reference switch complete	page 4-111
—continued—	

Table 4-5 (continued)
Fac ESI alarms

Alarm	See
Reference switch fail	page 4-112
Rx AIS	page 4-113
Timing reference interface fail	page 4-114
Tx AIS	page 4-115
Undefined sync status message	page 4-118
—end—	

Table 4-6
Fac HDSL alarms

Alarm	See
ES threshold exceeded	page 4-119
Loopback	page 4-119
Loss of Sync	page 4-119
Margin threshold exceeded	page 4-119

Table 4-7
Fac OC-12 alarms

Alarm	See
Inter-ring both feeds fail	page 4-120
Inter-ring forced switch request	page 4-121
Inter-ring protection switch complete	page 4-122
RX inter-ring secondary feed fail	page 4-123
TX loss of inter-ring secondary feed	page 4-124

Table 4-8
Fac OC-3/OC-12 alarms

Alarm	See
Laser bias current	page 4-125
Line RFI	page 4-126
Line Rx CV threshold 1, 2, Line Rx ES threshold 1, 2, Line Rx SES threshold 1, 2, Line Rx UAS threshold 1, 2, Sect Rx CV threshold 1, 2, Sect Rx ES threshold 1, 2, Sect Rx SES threshold 1, 2, Sect Rx SEFS threshold 1, 2	page 4-127
Loss of frame	page 4-135
Rx AIS	page 4-139
Rx loss of signal	page 4-140
Section Rx optical power threshold	page 4-144
Signal degrade	page 4-145
Signal fail	page 4-148
STS1 Rx AIS	page 4-152
STS1 Rx loss of pointer	page 4-156
STS1 Rx unequipped	page 4-162

Table 4-9
Fac STS1 alarms

Alarm	See
Line Rx BCV threshold 1, 2 Line Rx BES threshold 1, 2 Line Rx BSES threshold 1, 2 Line Rx CV threshold 1, 2 Line Rx ES threshold 1, 2 Line Rx SES threshold 1, 2 Line Rx UAS threshold 1, 2	page 4-163
Loopback	page 4-167
Rx bipolar violation >10E-3	page 4-168
Rx loss of frame	page 4-171
Rx loss of pointer	page 4-174
Rx loss of signal	page 4-175
Rx Line AIS	page 4-178
Rx RFI	page 4-179
STS1 Rx AIS	page 4-180

Table 4-10
Fac TIC alarms

Alarm	See
PRI link OOS	page 4-183
STS1 Rx RFI	page 4-184
STS1 Rx unequipped	page 4-185
TR-08 System [1 … 21] far end major	page 4-191
TR-08 System [1 … 21] loss of Rx DDL	page 4-192
TR-08 System [1 … 21] Rx fail	page 4-199
VT Path signal label mismatch	page 4-200
VT Rx AIS	page 4-201
VT Rx loss of pointer	page 4-208
VT Rx RFI	page 4-213
VT Rx unequipped	page 4-216

Fac COMM
Faulty path

Probable cause

This alarm is raised in a GR-303 configuration against an EOC, CSC, or TMC channel, when the active and standby path cannot carry traffic, and it fails to switch to the standby path. The alarm appears when the performance of the communication medium falls below the expected value. This is indicated by cyclic redundancy check (CRC) errors or aborted frames at the physical layer. All LAPD links of this path may be out of service.

This alarm can be caused by one or more of the following conditions:

- DS1 equipment problems, such as loss of signal or connection errors
- defective transport interface card (TIC)
- defective TXC OC-3/OC-12 optical interface or access interface card
- defective DS1/VT mapper at the FCOT
- defective processor circuit pack
- incorrect provisioning of the DS1ource
- link assignment is provisioned incorrectly in the OPC Facility Assignment Manager tool
- incorrect state of the IDT or CSC/EOC/TMC paths at the Subscriber Carrier Module-100 Access (SMA)
- equipment between the SMA and the FCOT is not provisioned consistently with the SMA and FCOT (for example, line coding and frame format for a fiber mux)
- STS routing or VT routing mismatch

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

—continued—

Fac COMM
Faulty path (continued)

Action

Step	Action
1	Clear any alarms raised against an TXC, OC-3 or OC-12 optical interface, DS1/VT mapper, access interface card (AIC), or transport interface card (TIC).
2	Clear the FCOT network element of any DS1 facility alarms.
3	Check that the Subscriber Carrier Module-100 Access (SMA) connected to this AccessNode has not been taken off line.
4	Check that both the primary and standby paths at the SMA are not manual busy or inhibited.
5	Check that the line coding is correctly set for extended superframe (ESF) for the DS1s carrying both the primary and standby paths. Also, ensure that the frame format for the DS1 is the same as that provisioned in Table LTCPSINV at the SMA.
6	Make sure the physical DS1 connection matches the provisioned information in SMA table RDTINV. Also, verify that Tx and Rx are not swapped.
7	Verify that the host name in the OPC Host Provisioning Manger tool is the same as the host name in Table OFCENG at the SMA (pos office_clli_name).
8	Verify that the GR-303 DS1 circuits have the correct hostname in the OPC Facility Assignment Manager tool, and that the first two links are numbered one and two.
9	At the RFT, verify which STS the GR-303 circuits are on, and ensure that the associated VT1.5s (one and two) are in service.
10	Check that the facilities for DS1s carrying both the primary and standby paths are in service.
11	Check the clock source for the FCOT and RFT. The RFT must be looptimed, while the FCOT must be freerun or ESI timed.
12	Check the SMA for any carrier alarms at the trunks carrier level (TRKS;CARRIER;POST_SMA_x where x is the SMA number).
13	Verify the signaling path from the SMA to the FCOT by operating DS1 facility loopbacks towards the SMA, and executing the external continuity test on the out-of-service link.
14	Check the optical performance statistics at both the FCOT and RFT. If there are performance errors, look them up in this chapter, and proceed as described.
15	Check the DS1 performance statistics at the RFT. If there are performance errors, look them up in this chapter, and proceed as described.
16	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac COMM
No active path

Probable cause

The LAPD links composed of both primary and standby paths are in service, but there is no activity.

This alarm can be caused by any of the following conditions:

- DS1 equipment problems, such as loss of signal or connection errors
- defective OC-3/OC-12 optical interface or access interface card
- defective DS1/VT mapper at the FCOT
- defective processor circuit pack
- incorrect provisioning of the OC-3/OC-12, DS1 or clock source

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Clear any alarms raised against an OC-3 or OC-12 optical interface, DS1/VT mapper, or access interface card (AIC).
2	Clear the FCOT network element of any DS1 facility alarms.
3	Check that the Subscriber Carrier Module-100 Access (SMA) connected to this AccessNode is not off line.
4	Check that both the primary and standby paths at the SMA are not manual busy or inhibited.
5	Check that the line coding is correctly set for extended superframe (ESF) for the DS1s carrying both the primary and standby paths.
6	Check the clock source for the FCOT and RFT. The RFT must be looptimed, while the FCOT must be freerun or ESI timed.
7	Check the SMA for any carrier alarms.
8	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac COMM
OMC link fail

Probable cause

The network element cannot communicate through the DS1 facility to the far-end network element. This alarm is caused by any one of the following faults:

- DS1 facility problems, such as a loss of signal or loss of frame, resulting from cut lines or degraded timing synchronization
- lack of end-to-end connectivity
- defective DS1/VT mapper at either the local or far-end network element
- defective timing and cross-connect (TXC) card at either the local or far-end network element
- defective transport interface card (TIC) at either the local or far-end network element
- defective access interface card (AIC) at either the local or far-end network element
- defective processor card at either the local or far-end network element
- defective maintenance interface card (MIC)

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Verify that there is end-to-end continuity over the facility. ***Note:*** For details, see the procedure for verifying DS1 signal continuity in *Commissioning and Testing*, Volume 3.
2	Verify timing synchronization provisioning and the clock source selection. ***Note:*** For details, see the procedures for provisioning TXC timing parameters in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning,* Volume 4B.
3	From the detailed alarm screen record the OMC link number, and the DS1 group and port number for each OMC link fail alarm that is associated with the network element.

—continued—

Fac COMM
OMC link fail (continued)

Step	Action
4	Choose an OMC link fail alarm to work on (if you recorded more than one OMC alarm in step 3).
5	Check for DS1 facility alarms or alerts that are associated with the DS1 carrying the OMC link. ***Note:*** Check the DS1 facility alarms or alerts at both the local or far-end network elements.

If there are	Then
DS1 facility alarms or alerts	clear the alarms using the appropriate procedures in this manual. Go to step 6.
no DS1 facility alarms or alerts	go to step 7.

6 Determine if the *OMC link fail* alarm clears.

If the alarm	Then
clears	if more OMC link fail alarms exist, go to step 4, otherwise, end the procedure.
persists	go to step 7.

7 Check for alarms against the DS1/VT mapper that is associated with the OMC link you are working on.

Note: You recorded the group number of the DS1/VT mapper in step 3. Check for DS1/VT mapper alarms at both the local and far-end network elements.

If there are	Then
DS1/VT mapper alarms	clear the alarms using the appropriate procedures in this manual. Go to step 8.
no DS1/VT mapper alarms	go to step 9.

8 Determine if the *OMC link fail* alarm clears.

If the alarm	Then
clears	if more OMC link fail alarms exist, go to step 4, otherwise, end the procedure.
persists	go to step 9.

—continued—

Fac COMM
OMC link fail (continued)

Step	Action
9	Check for TXC, TIC, AIC, MIC, and processor card alarms at both the local and far-end network element: **alarms.**↵

If TXC, TIC, AIC, MIC or processor alarms	Then
exist	clear the alarms using the appropriate procedures in this manual. Go to step 10.
do not exist	if more OMC link fail alarms exist, go to step 4, otherwise, go to step 11.

10 Determine if the *OMC link fail* alarm clears.

If the alarm	Then
clears	if more OMC link fail alarms exist, go to step 4, otherwise, end the procedure.
persists	go to step 11.

11 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac COMM
OMC performance degraded

Probable cause

The performance of the communication medium falls below the expected value. This is indicated by the occurrence of CRC errors and/or aborted frames at the physical layer. This alarm may be caused by any of the following faults:

- degraded DS1 facility connections resulting from poor connections or degraded timing synchronization
- a defective DS1/VT mapper at the local or far-end network element
- a defective timing and cross-connect (TXC) card at the local or far-end network element
- a defective transport interface card (TIC) at the local or far-end network element
- a defective access interface card (AIC) at the local or far-end network element
- a defective maintenance interface card (MIC) at the local or far end network element
- a defective processor card at the local or far-end network element
- loose connections

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	From the detailed alarm screen record the OMC link number, and the DS1 group and port number for each OMC link fail alarm that is associated with the network element.
2	Choose an OMC link fail alarm to work on (if more than one exists).

—continued—

Fac COMM
OMC performance degraded (continued)

Step	Action

3 Check for DS1 facility alarms or alerts that are associated with the DS1 carrying the OMC link.

Note: Check the DS1 facility alarms or alerts at both the local or far-end network elements.

If there are	Then
DS1 facility alarms or alerts	clear the alarms using the appropriate procedures in this manual. go to step 4.
no DS1 facility alarms or alerts	go to step 5.

4 Determine if the *OMC performance degraded* alarm clears.

If the alarm	Then
clears	if more OMC performance degraded alarms exist, go to step 2, otherwise, end the procedure.
persists	go to step 5.

5 Verify timing synchronization provisioning and the clock source selection.

Note: For details, see the procedures for provisioning TXC timing parameters in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning,* Volume 4B.

6 Check for alarms against the DS1/VT mapper that is associated with the OMC link you are working on.

Note: You recorded the group number of the DS1/VT mapper in step1.

7 Check for DS1/VT mapper alarms at both the local and far-end network elements.

If there are	Then
DS1/VT mapper alarms	clear the alarms using the appropriate procedures in this manual. Go to step 8.
no DS1/VT mapper alarms	go to step 9.

—continued—

Fac COMM
OMC performance degraded (continued)

Step	Action
8	Determine if the *OMC performance degraded* alarm clears.

If the alarm	Then
clears	if more OMC performance degraded alarms exist, go to step 2, otherwise, end the procedure.
persists	go to step 9.

9 Check for TXC, TIC, AIC, MIC, and processor card alarms at both the local and far-end network element:

alarms.↵

If TXC, TIC, AIC, MIC or processor alarms	Then
exist	clear the alarms using the appropriate procedures in this manual. Go to step 10.
do not exist	go to step 11.

10 Determine if the OMC link fail alarm clears.

If the alarm	Then
clears	if more OMC performance degraded l alarms exist, go to step 2, otherwise, end the procedure.
persists	go to step 11.

11 Verify the integrity of all connections.

If the alarm	Then
clears	end the procedure.
persists	if more OMC performance degraded alarms exist, go to step 2, otherwise, go to step 12.

12 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac COMM
SONET DCC link fail

Probable cause

The shelf processor cannot communicate through the SONET data communication channel (SDCC) due to one of the following conditions:

- the far end processor is rebooting or downloading a software load from the OPC
- there is a crossed fiber between channels, or a cut fiber
- the OC-3 or OC-12 optical interface circuit pack is defective
- the maintenance interface circuit pack is defective or missing
- the far end processor is defective

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Open the OPC Event Browser tool on the OPC and check for an SDA353 or SDA 369 log, which indicate a problem with software download to the far-end NE processor. If one of these logs is present, look up the log in *Log Report Manual*, 323-3001-840, in *Maintenance*, Volume 5B. If a software download is in progress, indicated by an SDA701 log, wait for several minutes to see if the alarm clears or if one of the download trouble logs is raised (SDA353 or SDA 369). If one of these logs is raised, look up the log in *Log Report Manual*, 323-3001-840, *Maintenance*, Volume 5B.
2	Verify all origination and termination points for the fiber-optic cables connected to the OC-3 or OC-12 circuit packs. Fibers from the G1 (working) optics at the FCOT must connect to the G1 (working) optics at the RFT. The proper connection is from receiver (Rx) to transmitter (Tx).
3	Check for facility alarms raised against the OC-3 or OC-12 optical facility. If there are optical facility alarms, look them up in this document and clear them accordingly.
4	Check for equipment alarms raised against the maintenance interface circuit pack (MIC). If there are MIC equipment alarms, look them up in this document and clear them accordingly.

—continued—

Fac COMM
SONET DCC link fail (continued)

Step	Action
5	Check for equipment alarms raised against the shelf processors. If there are Proc equipment alarms, look them up in this document and clear them accordingly.
6	If this alarm persists, there may be an undetectable fault associated with the circuit packs. Replace the following circuit packs one at a time until the alarm clears. To replace a circuit pack, follow the procedures in *Log Report Manual*, 323-3001-840, in *Maintenance*, Volume 5B. • replace the MIC at the local network element (where this alarm was raised) • replace the MIC at the far-end network element • replace the processor at the local network element • replace the processor at the far-end network element. • replace the working OC-3 or OC-12 optical interface
7	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac COMM
SONET DCC performance degraded

Probable cause

The performance of the communication medium has fallen below the expected value. This is indicated by the cyclic redundancy check (CRC) errors or aborted frames at the physical layer.

This alarm can be caused by any of the following conditions:

- defective OC-3/OC-12 optical interface or access interface card
- defective processor circuit pack at either network element
- defective maintenance interface circuit pack
- a loose fiber connection

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Check the connection of the optical fibers at each network element.
2	Check for alarms raised against the OC-3 or OC-12 optical interfaces at each network element, and clear them.
3	Check for alarms raised against the maintenance interface circuit pack at each network element, and clear them.
4	Check for alarms raised against the processor at each network element, and clear them.
5	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
CSU line loopback
Facility loopback
Network loopback
Terminal loopback

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543 for information on the following AccessNode Express alarms and the appropriate alarm clearing procedures.

The following alarms are AccessNode Express DS1 facility alarms.

- CSU line loopback
- Facility loopback
- Network loopback
- Terminal loopback

—end—

Fac DS1
High traffic threshold exceeded

Probable cause

The number of failed DS1s per host falls above the high percentage that was preset using a command line interface (CI) tool.

Impact

This is a critical, service-affecting (C, SA) alarm.

Action

Step	Action
1	Verify that all DS1s connected to the IG in question are in service. If any are out of service, attempt to bring them into service.
2	If the alarm is still active, verify that the traffic alarm thresholds are set correctly (see *Line Card Provisioning Procedures*, 323-3001-315, in *Operations, Administration, and Provisioning*, Volume 4B).

—end—

Fac DS1
Line Rx CV threshold 1, 2, Line Rx ES threshold 1, 2, Line Rx SES threshold 1, 2

Probable cause

For CV: the count of bipolar coding violations has exceeded the set threshold.

For ES: in a one-second period, one or more line coding violations have been detected.

For SES: in a one-second period, more than 44 line coding violations have been detected. This corresponds to a LineCV error rate of 1x10E-6.

The above line Rx threshold crossings are typically due to a faulty DS1 input cable or connection, or a problem with the source of the incoming DS1 signal.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Try to isolate the fault by checking DS1 cables, connectors and signals at the receiving end, then at the transmitting end, as described in the following procedure.

Step	Action
1	In the I/O portion of the common-equipment shelf, locate the DS1 Input card associated with the facility that is reporting this alarm.

CAUTION
Possible loss of service
While inspecting DS1 cables and connectors, do not disconnect the DS1 cable from the DS1 input card, as this will cause a loss of service on up to 14 DS1 facilities.

—continued—

Fac DS1
Line Rx CV threshold 1, 2,
Line Rx ES threshold 1, 2,
Line Rx SES threshold 1, 2 (continued)

Step	Action

2 Inspect the DS1 cable from the DSX cross-connect to the DS1 input card. Make sure the cable is not damaged and that it is properly connected and secured to the connector on the DS1 input card.

If the cable	Then
appears damaged	go to step 5.
good	go to step 3.

3 At the DS1 cross-connect, use a receiver test set to test the incoming signal for excessive errors.

If the incoming signal	Then
has excessive errors	go to step 4.
is free of errors	go to step 5.

4 The DS1 signal source appears to be faulty. Check all cables, connections and signals at the source and repair as required.

If the alarm	Then
persists	go to step 7.
clears	end the procedure.

5

CAUTION
Loss of service
Disconnecting the DS1 cable from the DS1 input card, will cause a loss of service on up to 14 DS1 facilities.

The DS1 cable from the DSX cross-connect to the DS1 input card appears to be faulty. Replace this DS1 cable.

If this alarm	Then
clears	end the procedure.
persists	go to step 6.

—continued—

Fac DS1
Line Rx CV threshold 1, 2,
Line Rx ES threshold 1, 2,
Line Rx SES threshold 1, 2 (continued)

Step	Action
6	The DS1 input card appears to be faulty. Replace the DS1 input card, as described in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C, then return to this procedure.

If the alarm	Then
persists	go to step 7.
clears	end the procedure.

7	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
Loopback

Probable cause

A DS1 facility is looped back for testing.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

No action is required. If you want to release the loopback on the DS1 facility, use the following procedure.

Step	Action
1	From any FWPUI screen, display the alarm report for this alarm: **almrpt <alarm #>**↵ where <alarm #> is the number on the screen which corresponds to the one-line alarm report. *The alarm report appears.*
2	Determine from the alarm report which facility has the alarm condition.
3	From the alarm screen, display the DS1 facility screen: **fa ds1 <group> <port>**↵ where <group> is the number of the DS1 group from step 2. <port> is the number of the DS1 port from step 2.
4	Release the loopback: **loopback re**↵ *The loopback is released.*
5	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
Low traffic threshold exceeded

Probable cause

The number of failed DS1s per host falls below the low percentage that was preset using a command line interface (CI) tool.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Verify that all DS1s connected to the IG in question are in service. If any are out of service, attempt to bring them into service.
2	If the alarm is still active, verify that the traffic alarm thresholds are set correctly (see *Line Card Provisioning Procedures*, 323-3001-315, in *Operations, Administration, and Provisioning*, Volume 4B).

—end—

Fac DS1
Path Rx CV threshold 1, 2
Path Rx ES threshold 1, 2
Path Rx SAS threshold 1, 2
Path Rx SES threshold 1, 2
Path Rx UAS threshold 1, 2

Probable cause

Threshold crossing of DS1 RX performance monitoring parameter due to:

- bad DS1 input cable or connector
- problem with the source of the DS1 signal
- faulty DS1 mapper circuit pack
- faulty DS1 switcher
- faulty I/O card

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Note 1: It is assumed that these thresholds have been provisioned as alarms and are turned ON (activated). If they are not provisioned as alarms, these alarm points will show up as performance alerts.

Note 2: These alarms indicate that errors in excess of a provisioned level have been observed. Threshold crossing alarms will automatically clear at the end of the provisioned interval.

Action

Note 1: Before replacing a circuit pack, try to clear the alarm by re-installing the same circuit pack (see *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C), ensuring the circuit pack is protected before removing and reseating it.

Note 2: This procedure is service affecting.

—continued—

Fac DS1
Path Rx CV threshold 1, 2
Path Rx ES threshold 1, 2
Path Rx SAS threshold 1, 2
Path Rx SES threshold 1, 2
Path Rx UAS threshold 1, 2 (continued)

Step	Action
1	Display the performance monitoring screen by entering: **perfmon**↵ *The performance monitoring screen appears.* If no errors are occurring, no immediate action is required. The alarm will clear at the end of the provisioned interval.
2	From the network element user interface, perform a manual switch on the DS1/STS mapper circuit pack by entering: **protectn** ↵ **dtlprot ds1** ↵ **manual op <circuit pack group>** ↵ **yes** ↵ where <circuit pack group> is the specified circuit pack. See *Provisioning and Operations Procedures*, 323-3001-310, in Operations, Administration and Provisioning, Volume 4B for more details.
3	If the problem is not corrected, go to step 4; if the problem is corrected, then replace the defective DS1/STS mapper circuit pack. See *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C, for replacement instructions.
4	Release the manual switch by entering: **protectn** ↵ **dtlprot ds1** ↵ **manual re <circuit pack group>** ↵ **yes** ↵ where <circuit pack group> is the one used at step 2.
5	In the top level of the shelf, locate the DS1 Input circuit pack allocated to the port reporting the errors. Examine the DS1 cable connected to its connector. Make sure that the correct connector is used and is well secured. If the cable is split or damaged, replace it. If the problem persists, go to step 6.

—continued—

Fac DS1
Path Rx CV threshold 1, 2
Path Rx ES threshold 1, 2
Path Rx SAS threshold 1, 2
Path Rx SES threshold 1, 2
Path Rx UAS threshold 1, 2 (continued)

Step	Action
6	Unplug the DS1 cable from the DS1 Input circuit pack and connect it to a DS1 receiver test set. Verify that a DS1 signal is present on that cable and that the test set does not detect any errors. If there are no errors, then re-connect the DS1 cable and go to step 8. Otherwise, continue to step 7.
7	If errors were detected at the DS1 Input circuit pack (in step 2) verify the signal at the source with the DS1 test set. If there are errors, then the source generating the DS1 signal should be repaired. If there are no errors, continue with step 8.

CAUTION
Loss of Service
When you remove a DS1 Input circuit pack, you lose 14 DS1s associated with that pack.

8	At this point, the DS1 cable and the DS1 signal source have been verified. If errors are still occurring, then replace the DS1 Input circuit pack attributed to this port. See *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C, for replacement instructions. If the problem persists, go to step 9.
9	With the DS1 cable connected to the DS1 Input circuit pack, go to the source of the DS1 signal. With the DS1 test set, monitor the DS1 signal. If the test set monitors an error-free signal, the cable must be replaced or repaired. If the signal is not error-free, the equipment generating the DS1 signal will have to be repaired.
10	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
PRI link OOS

Probable cause

Data Direct's ISDN primary link interface (PRI) is out of service (OOS).

Impact

This is a major, service affecting alarm (M, SA).

Action

Step	Action
1	Display the DS1 facility for the PRI links and make sure the status is in service.
2	If the status is OOS, or if the facility does not exist, put the facility in service. For directions, see *Provisioning and Operations Procedures*, 323-2001-310, in *Operations, Administration, and Provisioning*, Volume 4B.
3	If the problem persists, contact your next level of support.

—end—

Fac DS1
Rx AIS

Probable cause

There is an alarm condition at the far-end (transmitting) DS1 that is affecting the signal being received.

Note: If the alarm has AX in the Sh column, this is an AccessNode Express (ANX) alarm raised on a voice module. See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on this alarm.

Example ANX alarm:

```
Alm   Class   Sh    Type  Unit  Reason    Severity
12    Fac     AX12  DS1         Rx AIS    M,SA
```

Impact

This is a major, service-affecting (M, SA) alarm. The warning status indicates that the problem is with the transmitted signal from the far-end site.

Action

Log in to the network element user interface at the far-end network element. Check for a DS1 equipment or facility alarm. Look up the alarm in this document, and proceed accordingly.

For details on how to log in to the network element user interface and view alarms, see “Displaying alarms” on page 1-2.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
Rx babbling

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543 for information on this AccessNode Express alarm and the appropriate alarm clearing procedure.

—end—

Fac DS1
Rx bipolar violation > 10E-3

Probable cause

The transmitted signal from the far-end site has degraded to the point where bipolar code violations are greater than 10^{-3}, or the DS1 power level at the far-end site is not sufficient for the length of cable. Violations are typically a problem with the transmitting equipment, but may be caused by faulty cabling or circuitry at the receiving end.

Note: If the alarm has AX in the Sh column, this is an AccessNode Express (ANX) alarm raised on a voice module. See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on this alarm.

Example ANX alarm:

```
Alm   Class   Sh    Type  Unit  Reason    Severity
12    Fac     AX12  DS1         Rx AIS    M,SA
```

Impact

This is a major, service-affecting (M, SA) alarm. Traffic associated with the DS1 facility is affected.

Action

Step	Action

1 Check the far-end site (network element or external equipment) for a DS1 equipment or facility alarm.

If	Then
there is a DS1 equipment or facility alarm	look up the alarm in this document, and proceed accordingly.
there are no DS1 equipment or facility alarms	go to step 2.

—continued—

Fac DS1
Rx bipolar violation > 10E-3 (continued)

Step	Action
2	At the far-end site, ensure that the line build-out is properly set for the length of cable. To check the line build-out (LBO) range at the far-end site, enter: **fa ds1 <group> <port>**↵ where <group> is the DS1 group number: see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15 for values. <port> is the number of the DS1 port: **1** to **14**. *The DS1 facility screen appears.*

If the LBO is	Then
correct	go to step 3.
not correct	change the LBO setting. See *Provisioning and Operations Procedures*,323-3001-310, in *Operations, Administration, and Provisioning,* Volume 4B, for DS1 facility provisioning instructions.

3 Replace the affected DS1/VT mapper circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

If the alarm	Then
persists	continue with this procedure at step 4.
clears	end the procedure.

4 At the near-end site (receiving end), check the cable between the DS1 Input card and the cross connect for physical damage.

If the cable is	Then
good	go to step 5.
damaged	replace the cable.

—continued—

Fac DS1
Rx bipolar violation > 10E-3 (continued)

Step	Action

5 This step removes up to 14 DS1s from service.

CAUTION
Loss of service
There are up to 14 DS1s associated with each DS1 group. Taking a DS1 group out of service will result in a loss of service on14 DS1s.

From the Network Element Status screen, take the affected DS1 group out of service:

eq ds1 <group>↵

chgstate oos↵

yes↵

where

<group>	is the number of the DS1 group: see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15 for values.

6 Replace the DS1 Input card as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

If	Then
the alarm clears	end the procedure.
the alarm persists	go to step 7.

7 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
Rx bipolar violation > 10E-4

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543 for information on this AccessNode Express alarm and the appropriate alarm clearing procedure.

—end—

Fac DS1
Rx loss of frame

Probable cause

The DS1 is unable to detect the provisioned framing format for the incoming DS1 signal. The frame format is not set the same for each end of the facility, or the framing is corrupted.

Note 1: If this alarm occurs for all DS1 facility ports, the DS1 frame format may be incorrectly provisioned. See facility provisioning procedures *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B.

Note 2: If the alarm has AX in the Sh column, this is an AccessNode Express (ANX) alarm raised on a voice module. See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on this alarm.

Example ANX alarm:

```
Alm   Class   Sh    Type  Unit  Reason    Severity
12    Fac     AX12  DS1         Rx AIS    M,SA
```

Impact

This is a major, service-affecting (M, SA) alarm. Traffic associated with the DS1 facility is affected.

Action

Step	Action

1 Check the far-end (network element or external equipment) for a DS1 equipment or facility alarm.

If	Then
there is a DS1 equipment or facility alarm	look up the alarm in this document, and proceed accordingly.
there are no DS1 equipment or facility alarms	go to step 2.

—continued—

Fac DS1
Rx loss of frame (continued)

Step	Action

2 At each end of the DS1 facility, ensure that the frame format is set the same. To check the frame format, enter:

fa ds1 <group> <port>↵

where

<group>	is the DS1 group number: see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15 for values.
<port>	is the number of the DS1 port: **1** to **14**.

The DS1 facility screen appears.

If the frame formats are	Then
set the same	go to step 3.
not the same	change the frame format. See *Provisioning and Operations*, 323-3001-310, in *Operations, Administration, and Provisioning,* Volume 4B, for DS1 facility provisioning instructions.

3 Replace the affected DS1/VT mapper circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

If the alarm	Then
persists	go to step 4.
clears	end the procedure.

4 At the near-end site (receiving end), check the cable between the DS1 Input card and the cross connect for physical damage.

If the cable is	Then
good	go to step 5.
damaged	replace the cable.

—continued—

Fac DS1
Rx loss of frame (continued)

Step	Action

5 This step takes up to 14 DS1s out of service.

CAUTION
Loss of service
There are up to 14 DS1s associated with each DS1 group. Taking a DS1 group out of service will result in a loss of service on 14 DS1s.

From the Network Element Status screen, take the affected DS1 group out of service.

eq ds1 <group>↵

chgstate oos↵

yes↵

where

<group>	is the number of the DS1 group: see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15 for values.

6 Replace the DS1 Input card as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

If	Then
the alarm clears	end the procedure.
the alarm persists	go to step 8.

7 If the alarm persists, replace the OC-12 circuit pack where the failure is reported. See *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

8 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
Rx loss of signal

Probable cause

A signal was not detected on the DS1 line coming in to the equipment.

Note: If the alarm has AX in the Sh column, this is an AccessNode Express (ANX) alarm raised on a voice module. See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on this alarm.

Example ANX alarm:

```
Alm   Class   Sh    Type  Unit  Reason    Severity
12    Fac     AX12  DS1         Rx AIS    M,SA
```

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Check the far-end site (network element or external equipment) for a DS1 equipment or facility alarm.

If	Then
there is a DS1 equipment or facility alarm	look up the alarm in this document, and proceed accordingly.
there are no DS1 equipment or facility alarms	go to step 2.

—continued—

Fac DS1
Rx loss of signal (continued)

Step	Action

2 At the downstream site (receiving end), check the cable between the DS1 Input card and the cross connect for physical damage.

If the cable is	Then
good	go to step 3.
faulty	replace the cable.

3 Replace the DS1 Input card as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

If the alarm	Then
clears	end the procedure.
persists	go to step 4.

CAUTION
Service Interruption
There are up to 14 DS1s associated with a DS1 input card. Removing the connector from a DS1 input card results in a loss of up to 14 DS1s to the corresponding DS1/VT mapper.

4 If the alarm persists, replace the affected DS1/VT mapper circuit pack as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

5 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
Rx yellow

Probable cause

There is an alarm condition downstream at the receiving DS1 equipment or facility.

Note: If the alarm has AX in the Sh column, this is an AccessNode Express (ANX) alarm raised on a voice module. See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on this alarm.

Example ANX alarm:

```
Alm   Class   Sh    Type  Unit  Reason    Severity
12    Fac     AX12  DS1         Rx AIS    M,SA
```

Impact

This is a warning, not service-affecting (w, nsa) alarm for information only.

Action

Check the downstream network element for a DS1 equipment or facility alarm. Look up the alarm in this document, and proceed accordingly.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
STS1 path CV threshold 1, 2
STS1 path ES threshold 1, 2
STS1 path SES threshold 1, 2
STS1 path UAS threshold 1, 2

Probable cause

The threshold of a DS1 Tx performance monitoring parameter has been crossed because of one of the following conditions:

- a defective DS1 STS mapper circuit pack (local or far end)
- a defective DS1 switcher
- a possible OC-3/OC-12 equipment or optical link failure

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Note 1: This procedure assumes that these alarms have been provisioned as alarms and are turned on. If this is not so, these alarm points show up as performance alerts. This procedure also assumes that DS1 parity error correction is enabled.

Note 2: These alarms indicate errors in excess of a provisioned level. Threshold crossing alarms automatically clear at the end of the provisioned interval.

—continued—

Fac DS1
STS1 path CV threshold 1, 2
STS1 path ES threshold 1, 2
STS1 path SES threshold 1, 2
STS1 path UAS threshold 1, 2 (continued)

Action

CAUTION
Service Affecting
This procedure is service affecting.

Step	Action
1	To make sure a facility fault is not causing the alarm, check the OC-3/OC-12 performance monitoring facility for excessive errors by entering: **perfmon**↵ **facperf <type> <circuit pack group>**↵ where <type> is **oc3** or **oc12**. <circuit pack group> is the channel carrying traffic. If an OC-3/OC-12 facility panel is not causing the alarm, go to step 2.
2	From the network element user interface, perform a manual switch on the DS1 STS mapper circuit pack by entering: **protectn**↵ **dtlprot ds1**↵ **manual op <circuit pack group>**↵ **yes**↵ where <circuit pack group> is the circuit pack with the alarm.

If the alarm	Then
clears	replace the defective STS mapper circuit pack. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. Go to step 3.
persists	go to step 4.

—continued—

Fac DS1
STS1 path CV threshold 1, 2
STS1 path ES threshold 1, 2
STS1 path SES threshold 1, 2
STS1 path UAS threshold 1, 2 (continued)

Step	Action
3	Release the manual switch by entering: **protectn**↵ **dtlprot ds1**↵ **manual re <circuit pack group>**↵ **yes**↵ where <circuit pack group> is the circuit pack from step 2.
4	If the alarm is still active, replace the DS1 switcher circuit pack. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
5	If the alarm is still active, complete the following substeps to replace the corresponding DS1 STS mapper circuit pack on the other OC-3/OC-12 terminal in the system: **a.** Log in to the other terminal. **b.** From the network element user interface, perform a manual switch on the DS1 STS mapper circuit pack by entering: **protectn**↵ **dtlprot ds1**↵ **manual op <circuit pack group>**↵ **yes**↵ where <circuit pack group> is the circuit pack corresponding to the circuit pack with the alarm.

If the alarm	Then
clears from the original terminal (check alarm points in Alarm Monitor)	replace the defective STS mapper circuit pack in the other terminal. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. Go to step 6.
persists	go to step 7.

—continued—

Fac DS1
STS1 path CV threshold 1, 2
STS1 path ES threshold 1, 2
STS1 path SES threshold 1, 2
STS1 path UAS threshold 1, 2 (continued)

Step	Action
6	Release the manual switch by entering: **protectn**↵ **dtlprot ds1**↵ **manual re <circuit pack group>**↵ **yes**↵ where <circuit pack group> is the circuit pack from step 5.
7	If errors still occur, perform a manual switch of the optics on the alarmed network element by entering: **protectn**↵ **dtlprot <type>**↵ **manual op <circuit pack group>**↵ **yes**↵ where <type> is **oc3** or **oc12**. <circuit pack group> is the working channel group number.

If the alarm	Then
clears	Replace the optical interface circuit pack. For directions, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. Go to step 8.
persists	Contact your next level of support.

—continued—

Fac DS1
STS1 path CV threshold 1, 2
STS1 path ES threshold 1, 2
STS1 path SES threshold 1, 2
STS1 path UAS threshold 1, 2 (continued)

Step	Action
8	Release the manual switch by entering: **protectn**↵ **dtlprot <type>**↵ **manual re <circuit pack group>**↵ **yes**↵ where <type> is **oc3** or **oc12**. <circuit pack group> is the circuit pack from step 7.

—end—

Fac DS1
STS1 Rx path trace failure

Probable cause

The system detected an error in the path trace information which accompanies each STS1 frame. One of the following reasons could cause this alarm:

- the upstream (transmitting) DS1/VT mapper is defective
- the upstream (transmitting) OC-3/OC-12 is defective
- the local OC-3/OC-12 is defective
- the local DS1/VT mapper is defective
- in a GR-303 or DS1 Tandem configuration, check for problems with the TIC at the remote network element.

If more than one STS1 path trace failure alarm is present at a network element, then a defective OC-3/OC-12 optical interface is likely the cause.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	From any network element FWPUI screen, display a list of active alarms and check for an OC-3/OC-12 equipment or facility alarm: **alarms**↵ *A summary list of alarms appears.*

If	Then
there is an OC-3/OC-12 alarm	go to step 3.
is no OC-3/OC-12 alarm	go to step 2.

Step	Action
2	Log in to the user interface at the upstream network element, display a list of active alarms, and check for an OC-3/OC-12 equipment or facility alarm.

If	Then
there is an OC-3/OC-12 alarm	go to step 3.
is no OC-3/OC-12 alarm	go to step 4.

—continued—

Fac DS1
STS1 Rx path trace failure (continued)

Step	Action

3 Look up the alarm in this document and proceed as instructed.

4 Perform a protection switch on the upstream DS1:

a. Display the DS1 protection switching screen:

pr;dtlprot ds1↵

The detailed protection screen appears.

b. Operate the manual switch:

manual op <group>↵
y↵

where

<group> is the DS1 circuit pack group from which traffic is being switched: see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15.

*The screen displays an asterisk * in the* `Manual` *column.*

If this alarm	Then
clears	go to step 7.
persists	go to step 5.

5 Perform a protection switch on the local DS1:

a. Log in to the local network element and display the DS1 protection switching screen:

pr;dtlprot ds1↵

The detailed protection screen appears.

b. Operate the manual switch:

manual op < group >↵
y↵***The screen displays an asterisk * in the*** **`Manual`** ***column.***

where

<group> is the DS1 circuit pack group from which traffic is being switched: see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15.

If this alarm	Then
clears	go to step 7.
persists	go to step 6.

—continued—

Fac DS1
STS1 Rx path trace failure (continued)

Step	Action

6 Perform a protection switch on the local (receiving) OC-3/OC12:

a. Log in to the local network element and display the OC-3/OC-12 protection switching screen:

pr;dtlprot <type>

where

<type> is the type of optical circuit pack: **oc3** or **oc12**.

The detailed protection screen appears.

b. Operate the manual switch:

manual op <group>↵
y↵

where

<group> is the OC-3/OC-12 circuit pack group from which traffic is being switched: **g1** or **g2**.

*The screen displays an asterisk * in the* `Manual` *column.*

If this alarm	Then
clears	go to step 7.
persists	go to step 8.

7 Replace the circuit pack from which service was switched, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

8 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
STS1 Rx RFI

Probable cause

The local node received a remote defect indication (RDI) because of a signal problem on the downstream equipment. The far end network element sent the RDI because it detected an STS1 alarm indication signal (AIS) or an STS1 loss of pointer (LOP) on the STS path signal.

Any of the following conditions can cause this alarm:

- The local DS1/VT mapper is transmitting an invalid or alarmed STS1 signal.
- The local OC-3/OC-12 optical interface is transmitting an invalid or alarmed STS1 signal.
- The downstream (receiving) DS1/VT mapper is not properly receiving the STS1 signal.
- The downstream OC-3/OC-12 optical interface is not properly receiving the STS1 signal.
- In a GR-303 or DS1 Tandem configuration, the downstream transport interface (TIC) card is not properly receiving the STS1 signal.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Log in to the user interface at the downstream (receiving) network element and display the list of active alarms: **alarms**↵ *The system displays a list of alarms in decreasing order of severity.*
2	Check for TIC, DS1, or OC-3/OC-12 alarms.

If a TIC, DS1 or OC-3/OC-12 alarm	**Then**
exists	look up the alarm in this document and proceed accordingly.
does not exist	go to step 3.

—continued—

Fac DS1
STS1 Rx RFI (continued)

Step	Action
3	Replace the local (transmitting) DS1/VT mapper at the network element where the STS1 Rx yellow alarm was originally displayed. For details see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If the alarm	Then
clears	end the procedure.
persists	if you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
STS1 Rx unequipped

Probable cause

The local DS1/VT mapper is not receiving an STS1 payload for one of the following reasons:

- all upstream DS1 STS1 facilities are out of service (OOS)
- the upstream DS1/VT mapper is defective
- in a GR-303 configuration, check for problems with the TIC at the remote network element

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Log in to the upstream network element user interface and display the DS1 facility screen: **fa ds1 < group > < port >**↵ where <group> is the group associated with STS1 alarm: see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15. <port> is the port number of the facility: **1** to **14**. *The DS1 facility screen appears with the STS1 state shown beside the heading* `STS1 Path Term State`*.*

—continued—

Fac DS1
STS1 Rx unequipped (continued)

Step	Action

If the STS1 state is	Then
OOS	go to step 2.
IS	go to step 3.
Trbl	go to step 3.

2 Change the state to in-service (IS):

chgstate is↵

The state of the facility and the STS1 path term change to in-service.

If this alarm	Then
clears	end the procedure.
persists	go to step 3.

3 Replace the upstream DS1/VT mapper, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

4 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
STS1 signal label mismatch

Probable cause

The terminations at the ends of an STS1 connection between two network elements (NE) are incompatible. For example, a DS1 on one NE is connected to a DS3 on another NE.

This alarm is raised at both ends of the connection.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	From the Connection Manager, verify the intended DS1-to-DS1 or DS3-to-DS3 connections are set up. The alarm was raised because these connections are misaligned.
2	Replace either the DS3/STS mapper circuit pack or the DS1/VT mapper circuit pack at one end of the connection, as indicated in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
3	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
VT Rx AIS

Probable cause

There is an alarm condition at the upstream (transmitting) DS1 or OC-3/OC-12.

In a GR-303 or DS1 Tandem configuration, there is an alarm condition at the upstream (transmitting) TIC.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	Log in to the user interface at the upstream (transmitting) network element and display the list of active alarms: ***Note:*** For details on displaying alarms, see *"Displaying alarms" on page 1-2*. **alarms**↵ *The system displays a list of alarms in decreasing order of severity.*
2	Check for a Fac DS1 Loopback alarm.

If a DS1 Loopback alarm	Then
exists	go to step 4.
does not exist	go to step 3.

3 Check for TIC, DS1 or OC-3/OC-12 alarms.

If a TIC, DS1 or OC-3/OC-12 alarm	Then
exists	look up the alarm in this document and proceed accordingly.
does not exist	go to step 7.

—continued—

Fac DS1
VT Rx AIS (continued)

Step	Action

4 From the Network Element Status screen, access the DS1 Facility screen:

fa ds1 < group > < port >↵

where

< group >	is the number of the DS1 group identified in step 2.
< port >	is the number of the DS1 port identified in step 2.

The DS1 facility screen appears.

5 Release the DS1 loopback:

loopback re↵

The loopback is released and the value to the right of the `Loopback` *heading reverts to* `None`*.*

6 Return the DS1 facility to service:

chgstate is↵

The value to the right of the heading `State` *changes.*

If state of the DS1 facility is now	Then
IS	verify that the VT Rx AIS alarm is cleared. If the alarm clears, end the procedure. If the alarm persists, then go to step 7.
IS-Trbl	go to step 7.
OOS	go to step 7.

7 Replace the local (receiving) DS1/VT mapper at the network element where the VT Rx AIS alarm was originally displayed.

If the alarm	Then
clears	end the procedure.
persists	if you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
VT Rx loss of pointer

Probable cause

The VT1.5 pointer is corrupted for one of the following reasons:

- the upstream (transmitting) DS1/VT mapper is defective
- the upstream (transmitting) OC-3/OC-12 optical interface is defective
- the local DS1/VT mapper is defective
- the local OC-3/OC-12 optical interface is defective
- in a GR-303 or DS1 Tandem configuration, check for problems with the TIC at the remote network element.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Log in to the upstream network element and check for OC-3/OC-12, DS1 or TIC equipment alarms.

If OC-3/OC-12, DS1 or TIC alarms	Then
are present	go to step 2.
are not present	go to step 3.

2	Look up the equipment alarm in this document and proceed to clear the alarm as instructed.

—continued—

Fac DS1
VT Rx loss of pointer (continued)

Step	Action
3	Perform a protection switch on the upstream DS1: **a.** Display the DS1 protection switching screen: **pr;dtlprot ds1**↵ *The detailed protection screen appears.* **b.** Operate the manual switch: **manual op <group>**↵ **y**↵ where <group> is the DS1 circuit pack group from which traffic is being switched: See "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15. *The screen displays an asterisk * in the* `Manual` *column.*

If this alarm	Then
clears	go to step 6.
persists	go to step 4.

—continued—

Fac DS1
VT Rx loss of pointer (continued)

Step	Action
4	At the upstream site, perform a protection switch on the transmitting OC-3 or OC-12:

a. Display the OC-3 or OC-12 protection switching screen:

pr;dtlprot <optical type>↵

where

<optical type> is the type of optical facility: **oc3** or **oc12**.

The OC-3 or OC12 detailed protection screen appears.

b. Check the values (`On` or `Off`) under the `Traffic Tx` column to determine which OC-3/OC-12 group (`G1` or `G2`) is actively transmitting.

c. Operate the manual switch on the transmitting OC-3/OC-12 group:

manual op <group>↵
y↵

where

<group> is the OC-3 or OC-12 circuit pack group from which traffic is being switched: **g1** or **g2**.

The screen displays a change of state between `G1` *and* `G2` *in the* `Traffic Tx Rx` *column.*

If this alarm	Then
clears	go to step 6.
persists	go to step 5.

—continued—

Fac DS1
VT Rx loss of pointer (continued)

Step	Action

5 Perform a protection switch on the local DS1 that reported this alarm:

a. Log in to the local network element and display the DS1 protection switching screen:

pr;dtlprot ds1↵

The detailed protection screen appears.

b. Operate the manual switch:

manual op < group >↵
y↵

where

< group >	is the DS1 circuit pack group from which traffic is being switched: see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15.

*The screen displays an asterisk * in the* `Manual` *column.*

If this alarm	Then
clears	go to step 6.
persists	go to step 7.

6 Replace the circuit pack from which service was switched, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

7 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
VT Rx RFI

Probable cause

The DS1 facility is indicating an alarm condition at the downstream (receiving) network element. Any of the following conditions can cause this alarm:

- The local DS1/VT mapper is transmitting an invalid or alarmed virtual tributary (VT) signal.
- The downstream (receiving) DS1/VT mapper is not properly receiving the VT signal.
- In a GR-303 or DS1 Tandem configuration, the downstream transport interface (TIC) card is not properly receiving the STS1 signal.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Note: If a protection bridge out card has just been removed, wait 30 seconds to see if this alarm clears by itself. If this alarm does not clear, then investigate the downstream (receiving) DS1 for alarms.

Step	Action
1	Log in to the user interface at the downstream (receiving) network element and display the list of active alarms: **alarms**↵ *The system displays a list of alarms in decreasing order of severity.*
2	Check for TIC, DS1, or OC-3/OC-12 alarms.

If a TIC, DS1 or OC-3/OC-12 alarm	Then
exists	look up the alarm in this document and proceed accordingly.
does not exist	go to step 3.

—continued—

Fac DS1
VT Rx RFI (continued)

Step	Action
3	Replace the local (transmitting) DS1/VT mapper at the network element where the VT Rx yellow alarm was originally displayed. For details see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If the alarm	Then
clears	end the procedure.
persists	if you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS1
VT Rx unequipped

Probable cause

The local DS1/VT mapper is not receiving a VT payload for one of the following reasons:

- the upstream DS1 facility is out of service (OOS)
- the upstream DS1/VT mapper is defective
- in a GR-303 or DS1 Tandem configuration, check for problems with the TIC at the remote network element.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Log in to the upstream network element user interface and display the DS1 facility screen: **fa ds1 <group> <port>**↵ where <group> is the circuit pack group number: See "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15. <port> is the corresponding port number for this facility: **1** to **14**. *The DS1 facility screen appears.*

If the DS1 facility state is	Then
IS	go to step 3.
OOS	go to step 2.
IS-Trbl	go to step 3.

—continued—

Fac DS1
VT Rx unequipped (continued)

Step	Action

2 Change the state of the facility to in-service (IS). (The corresponding DS1/VT mapper must be in service before a facility can go in service.)

chgstate is↵

y↵

The facility screen is updated with the new operating state.

If this alarm	Then
clears	end the procedure.
persists	go to step 3.

3 Perform a protection switch on the upstream DS1:

a. Log in to the upstream network element user interface and display the DS1 protection switching screen:

pr;dtlprot ds1↵

The detailed protection screen appears.

b. Operate the manual switch:

manual op <group>↵
y↵

where

<group>	DS1 circuit pack group from which traffic is being switched: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.

*The screen displays an asterisk * in the Manual column.*

If this alarm	Then
clears	go to step 4.
persists	go to step 5.

4 Replace the DS1/VT mapper from which service was switched, as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.

5 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
Frequency out of range

Probable cause

The DS3/STS mapper is

- receiving a bad clock reference from the active OC-3/OC-12 or ESI
- receiving a poorly clocked signal from the DS3 source

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Display the list of active alarms and check for ESI and OC-3/CO-12 alarms: **alarms**↵ *The list of active alarms appears.*

If there are	Then
ESI or OC-3/OC-12 alarms	use the appropriate alarm clearing procedures in this manual to clear the alarms. Go to step 3.
no ESI or OC-3/OC-12 alarms	go to step 2.

2 At the DS3 cross-connect, use a receiver test set to test the incoming signal for clocking problems.

If there are	Then
clocking problems	check all cables, connections and signals at the source and repair as required.
no clocking problems	go to step 4.

—continued—

Fac DS3
Frequency out of range (continued)

Step	Action
3	Determine if this `Frequency out of range` alarm is cleared.

If this alarm	Then
clears	end the procedure.
persists	go to step 2.

4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
Line FE CV threshold 1, 2
Line FE ES threshold 1, 2
Line FE SES threshold 1, 2
Line FE UAS threshold 1, 2

Probable cause

One of the following conditions caused a parameter threshold of STS-1 patch performance monitoring to be crossed:

- a degraded fiber connection
- a defective upstream optical interface circuit pack
- a defective local optical interface circuit pack

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action

1 Complete the instructions in the following table:

If an RX alarm is	Then
on G2	follow the instructions to clear G2 in the OC-3/OC-12 procedure “Line Rx CV threshold 1, 2” on page 4-127. If the alarm persists, go to step 2.
not on G2	go to step 2.

2 Complete the instructions in the following table:

If an RX alarm is	Then
on G1	follow the instructions to clear G1 in the OC-3/OC-12 procedure “Line Rx CV threshold 1, 2” on page 4-127. If the alarm persists, contact your Nortel Networks representative.
not on G1	contact your Nortel Networks representative.

—end—

Fac DS3
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2

Probable cause

For CV: the count of bipolar coding violations has exceeded the set threshold.

For ES: in a one-second period, one or more line coding violations have been detected.

For SES: in a one-second period, more than 44 line coding violations have been detected. This corresponds to a LineCV error rate of 1x10E-6.

The above line Rx threshold crossings are typically due to a faulty DS3 input cable or connection, or a problem with the source of the incoming DS3 signal.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Try to isolate the fault by checking DS3 cables, connectors and signals at the receiving end, then at the transmitting end, as described in the following procedure.

Step	Action
1	In the I/O portion of the common-equipment shelf, locate the DS3 I/O card associated with the facility that is reporting this alarm.

CAUTION
Possible loss of service
While inspecting DS3 cables and connectors, do not disconnect the DS3 cable from the DS3 I/O card, as this will cause a loss of service on the facility.

2	Inspect the DS3 cable from the DSX cross-connect to the DS3 I/O card. Make sure the cable is not damaged and that it is properly connected and secured to the connector on the DS3 I/O card.

If the cable	Then
appears damaged	go to step 5.
good	go to step 3.

—continued—

Fac DS3
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2 (continued)

Step	Action

3 At the DS3 cross-connect, use a receiver test set to test the incoming signal for excessive errors.

If the incoming signal	Then
has excessive errors	go to step 4.
is free of errors	go to step 5.

4 The DS3 signal source appears to be faulty. Check all cables, connections and signals at the source and repair as required.

If the alarm	Then
persists	go to step 7.
clears	end the procedure.

5

CAUTION
Loss of service
Disconnecting the DS3 cable from the DS3 I/O card, will cause a loss of service on the facility.

The DS3 cable from the DSX cross-connect to the DS3 I/O card appears to be faulty. Replace this DS3 cable.

If this alarm	Then
clears	end the procedure.
persists	go to step 6.

6 The DS3I/O card appears to be faulty. Replace the DS3 I/O card, as described in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, then return to this procedure.

If the alarm	Then
persists	go to step 7.
clears	end the procedure.

7 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
Loopback

Probable cause

A DS3 loopback has been operated and is currently active.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

This is a normal indication when the loopback is ON for testing purposes. If you want to release the loopback, use the following procedure.

Step	Action
1	To clear the alarm, release the loopback. **facility ds3 <group> <port #>** ↵ where <group> is the group number of the DS3: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15. <port #> is the number of the facility port: **1** to **3**, or **all** **loopback re <loopback type>** ↵ where <loopback type> is the type of loopback: **fac** or **term**
2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
Parity error rate >10E-6

Probable cause

A DS3/STS mapper has detected parity errors coming from an optical interface. The problem is one of the following:

- defective DS3/STS mapper
- defective OC-3/OC-12 optical unit

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Display the DS3 detailed protection screen to identify the DS3/STS mapper related to the alarm: **pr** ↵ **dtlprot ds3** ↵
2	Perform a forced switch: **forced op <group>** ↵ where <group> is the group number of the DS3: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.
3	If the alarm persists, replace the active OC-3/OC-12 optics circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.
4	If the alarm is cleared, replace the DS3/STS mapper. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.
5	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
Path Rx AISS threshold 1, 2
Path Rx CV threshold 1, 2
Path Rx ES threshold 1, 2
Path Rx SES threshold 1, 2
Path Rx SEFS threshold 1, 2
Path Rx UAS threshold 1, 2

Probable cause

For AISS: one or more short bursts of DS3 AIS (Blue Signal) events have been detected in one second.

For CV: the count of bipolar coding violations has exceeded the set threshold.

For ES: in a one-second period, one or more line coding violations have been detected.

For SES: in a one-second period, more than 44 Path coding violations have occurred, or one or more Out-of-Frame events has occurred, or one or more DS3 AIS events has occurred.

For SEFS: is a one-second period in which one or more out-of-frame events occurred.

The above path Rx threshold crossings are typically due to faulty DS3 cabling and connections, or a problem with the source of the incoming DS3 signal, or with DS3 circuit packs.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Try to isolate the fault by checking DS3 cables, connectors and signals at the receiving end, then at the transmitting end, and by checking DS3 equipment, as described in the following procedure.

—continued—

Fac DS3
Path Rx AISS threshold 1, 2
Path Rx CV threshold 1, 2
Path Rx ES threshold 1, 2
Path Rx SES threshold 1, 2
Path Rx SEFS threshold 1, 2
Path Rx UAS threshold 1, 2 (continued)

Step	Action

1 In the I/O portion of the common-equipment shelf, locate the DS3 I/O card associated with the facility that is reporting this alarm.

2

CAUTION
Possible loss of service
While inspecting DS3 cables and connectors, do not disconnect the DS3 cable from the DS3 I/O card, as this will cause a loss of service on the facility.

Inspect the DS3 cable from the DSX cross-connect to the DS3 I/O card. Make sure the cable is not damaged and that it is properly connected and secured to the connector on the DS3 I/O card.

If the cable	Then
appears damaged	go to step 5
good	go to step 3

3 At the DS3 cross-connect, use a receiver test set to test the incoming signal for excessive errors.

If the incoming signal	Then
has excessive errors	go to step 4.
is free of errors	go to step 5.

4 The DS3 signal source appears to be faulty. Check all cables, connections and signals at the source and repair as required.

If the alarm	Then
persists	go to step 9.
clears	end the procedure.

—continued—

Fac DS3
Path Rx AISS threshold 1, 2
Path Rx CV threshold 1, 2
Path Rx ES threshold 1, 2
Path Rx SES threshold 1, 2
Path Rx SEFS threshold 1, 2
Path Rx UAS threshold 1, 2 (continued)

Step	Action

5

CAUTION
Loss of service
Disconnecting the DS3 cable from the DS3 I/O card, will cause a loss of service on the facility.

The DS3 cable from the DSX cross-connect to the DS3 I/O card appears to be faulty. Replace this DS3 cable.

If this alarm	Then
clears	end the procedure.
persists	go to step 6.

6 The DS3I/O card appears to be faulty. Replace the DS3 I/O card, as described in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, then return to this procedure.

If the alarm	Then
persists	go to step 7.
clears	end the procedure.

—continued—

Fac DS3
Path Rx AISS threshold 1, 2
Path Rx CV threshold 1, 2
Path Rx ES threshold 1, 2
Path Rx SES threshold 1, 2
Path Rx SEFS threshold 1, 2
Path Rx UAS threshold 1, 2 (continued)

Step	Action

7 Verify that the DS3/STS mapper associated with the alarmed facility is functioning properly. From the network element status screen, perform a manual switch on the DS3/STS mapper:

pr ↵
dtlprot ds3 ↵
manual op <group> ↵

where

<group>	is the group number of the DS3: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.

The DS3 traffic is switched to the backup DS3/STS mapper.

If the alarm	Then
clears	go to step 8.
persists	go to step 9.

8 The DS3/STS mapper associated with this alarm, appears to be faulty. Replace the defective DS3/STS mapper, as described in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, then return to this procedure.

If the alarm	Then
clears	end the procedure.
persists	go to step 9.

9 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
Path Tx AISS threshold 1, 2
Path Tx CV threshold 1, 2
Path Tx ES threshold 1, 2
Path Tx SES threshold 1, 2
Path Tx SEFS threshold 1, 2
Path Tx UAS threshold 1, 2

Probable cause

For AISS: one or more short bursts of DS3 AIS (Blue Signal) events have been detected in one second.

For CV: the count of bipolar coding violations has exceeded the set threshold.

For ES: in a one-second period, one or more line coding violations have been detected.

For SES: in a one-second period, more than 44 Path coding violations have occurred, or one or more Out-of-Frame events has occurred, or one or more DS3 AIS events has occurred.

For SEFS: is a one-second period in which one or more out-of-frame events occurred.

For UAS: is a one-second period in which the path is unavailable.

The above path Tx threshold crossings are typically due to a faulty DS3/STS mapper, excessive optical facility errors or a faulty DS3 switcher.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Try to isolate the fault by first checking for optical performance monitoring alarms, or alerts. Then check the DS3/STS mapper and switcher, as described in the following procedure.

—continued—

Fac DS3
Path Tx AISS threshold 1, 2
Path Tx CV threshold 1, 2
Path Tx ES threshold 1, 2
Path Tx SES threshold 1, 2
Path Tx SEFS threshold 1, 2
Path Tx UAS threshold 1, 2 (continued)

Step	Action

1 Ensure that the alarm is not being caused by excessive optical errors. From the Network Element Status screen, display the facility performance statistics:

pm↵

facperf < type> < group >↵

where

<type>	is the type of optical facility: **oc3** or **oc12**.
<group>	is the group number of the active channel: **g1**or **g2**.

The facility performance monitoring screen appears.

If the optical facility	Then
has excessive errors	go to step 2.
is error free	go to step 3.

2 Look up the optical performance alarm/alert in this chapter, and clear it as instructed.

If this alarm	Then
clears	end the procedure.
persists	go to step 3.

—continued—

Fac DS3
Path Tx AISS threshold 1, 2
Path Tx CV threshold 1, 2
Path Tx ES threshold 1, 2
Path Tx SES threshold 1, 2
Path Tx SEFS threshold 1, 2
Path Tx UAS threshold 1, 2 (continued)

Step	Action

3 Verify that the DS3/STS mapper associated with the alarmed facility is functioning properly. From the network element status screen, perform a manual switch on the DS3/STS mapper:

pr ↵
dtlprot ds3 ↵
manual op <group> ↵

where

<group> is the group number of the DS3: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.

The DS3 traffic is switched to the backup DS3/STS mapper.

If the alarm	Then
clears	go to step 4.
persists	go to step 5.

4 The DS3/STS mapper associated with this alarm, appears to be faulty. Replace the defective DS3/STS mapper, as described in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, then return to this procedure.

If the alarm	Then
clears	end the procedure.
persists	go to step 5.

5 Replace the DS3 switcher as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, then return to this procedure.

If the alarm	Then
clears	end the procedure.
persists	go to step 6.

6 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
Rx AIS

Probable cause

The DS3 source at the far end of the DS3 cable is experiencing signal problems and is sending a DS3 Alarm Indication Signal (AIS).

Impact

This is a warning, service-affecting (w, SA) alarm.

Action

Check the DS3 equipment and the DS3 facility at the DS3 source located at the far end. Resolve any failures on the DS3 equipment or DS3 facilities.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
Rx bipolar violation > 10E-3

Probable cause

Bipolar violations have been detected on the incoming DS3 line due to:

- bad coaxial connector
- defective cable
- defective DS3 source equipment
- defective DS3 I/O card or DS3/STS mapper

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Verify if the DS3/STS mapper associated with the alarmed facility is functioning properly. Perform a manual switch on the DS3/STS mapper. **pr** ↵ **dtlprot ds3** ↵ **manual op <group>** ↵ where <group> is the group number of the DS3: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15. If the problem is corrected, replace the defective DS3/STS mapper and release the manual switch. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions. Otherwise, in the top level of the shelf, locate the DS3 I/O card allocated to the port reporting the Bipolar Violations. Examine the DS3 cable connected to its connector. Make sure that the correct connector is used and is well secured. If the cable is split or damaged, replace it. If the problem persists, proceed to step 2. **—continued—**

Fac DS3
Rx bipolar violation > 10E-3 (continued)

Step	Action

CAUTION
Possible loss of service
Disconnecting the DS3 cable in the next step will result in loss of service for that DS3 port.

2 Unplug the DS3 cable from the DS3 I/O card and connect it to a DS3 receiver test set. Verify that a DS3 signal is present on that cable and that the test set does not detect any errors.

If errors are detected replace the cable; otherwise, proceed to step 3.

3 In this step a DS3 I/O card is removed.

CAUTION
Possible loss of service
Make sure that the correct DS3 I/O card is removed. Removing the wrong unit will cause another DS3 signal to be lost. Replacing the DS3 I/O card will also cause the loss of the DS3 signal being sent on the “OUT” side of the concerned port.

Replace the DS3 I/O card attributed to this port. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

If the problem persists, proceed to step 4.

4 Reconnect the DS3 cable to the DS3 I/O card and go to the source of the DS3 signal. With the DS3 test set, monitor the DS3 signal.

If the test set monitors an error-free signal, the cable must be replaced or repaired. If the signal is not error-free, the equipment generating the DS3 signal will have to be repaired.

5 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
Rx loss of frame

Probable cause

The DS3 frame cannot be detected on the incoming DS3 due to:

- defective DS3 source equipment
- defective cable/connection
- defective DS3 I/O card
- defective DS3/STS mapper circuit pack

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Verify if DS3/STS mapper associated with alarmed facility is functioning properly. Perform a manual switch on the DS3/STS mapper. **pr** ↵ **dtlprot ds3** ↵ **manual op <group>** ↵ where <group> is the group number of the DS3: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15. If the problem is corrected, replace the defective DS3/STS mapper and release the manual switch. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions. Otherwise, in the top level of the shelf, locate the DS3 I/O card allocated to the port reporting the loss of frame. Examine the DS3 cable connected to its connector. Make sure that the correct connector is used and is well secured. If the cable is split or damaged, replace it. If the problem persists, proceed to step 2.

—continued—

Fac DS3
Rx loss of frame (continued)

Step	Action
2	Unplug the input DS3 cable from the DS3 I/O card and connect it to a DS3 receiver test set. Verify that a DS3 signal is present on that cable and that the test set does not detect any errors. If errors are detected, replace the cable; otherwise, proceed to step 3. If the problem persists (test set still detects errors) proceed to step 5.
3	Replace the DS3 I/O Interface circuit pack attributed to this port. **CAUTION** **Possible loss of service** Replacing the DS3 card will cause the loss of the DS3 signal of the concerned port while it is extracted. Make sure that the proper DS3 card is removed. Removing the wrong one will cause another DS3 signal to be lost.
4	If the problem persists, replace the DS3/STS mapper (NT7E08). See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.
5	Reconnect the DS3 cable to the DS3 I/O card and move to the source of the DS3 signal. With the DS3 test set, monitor the DS3 signal. If the test set monitors an error-free signal, the cable must be replaced or repaired. If the signal is not error-free, the equipment generating the DS3 signal will have to be repaired.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
Rx loss of signal

Probable cause

The DS3/STS mapper is not detecting any DS3 input signal due to:

- incoming Rx DS3 line fail (loss of signal)
- defective or missing DS3 I/O card

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Locate, in the top level of the shelf, the DS3 I/O card allocated to the port reporting the loss of signal. Examine the DS3 cable connected to its connector. Make sure that the correct connector is used and is well secured. If the cable is split or damaged, replace it. If the problem persists, proceed to step 2.
2	Unplug the DS3 cable from the DS3 I/O card and connect it to a DS3 receiver test set. Verify that a DS3 signal is present on that cable. If a signal is present, proceed to step 3. If no signal is present or if the signal is of poor quality, proceed to step 4.
	CAUTION **Possible loss of service** Replacing the DS3/IO card will cause loss of the DS3 signal of the concerned port while it is extracted. Make sure that the proper DS3 Interface circuit pack is removed. Removing the wrong one will cause another DS3 signal to be lost.
3	In this step a DS3 I/O card is replaced. Replace the DS3 I/O card attributed to this port. If the problem persists, proceed to step 5. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

—continued—

Fac DS3
Rx loss of signal (continued)

Step	Action
4	Reconnect the DS3 cable to the DS3 I/O card and go to the source of the DS3 signal. With the DS3 test set, monitor the DS3 signal. If a signal is present, the DS3 cable must be replaced or repaired. If no signal is present, the equipment generating the DS3 signal will have to be repaired.
5	Verify that the DS3 interconnect cable between the shelf and the DS3 Interconnect panel is secure. Use caution, the cable is also carrying other live DS3s.
6	If the LOS LED is still lit, replace the DS3/STS mapper. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.
7	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
STS1 path FE CV threshold 1, 2
STS1 path FE ES threshold 1, 2
STS1 path FE SES threshold 1, 2
STS1 path FE UAS threshold 1, 2

Probable cause

The threshold of an STS-1 path performance monitoring parameter has been crossed because of one of the following conditions:

- a degraded fiber connection
- a defective upstream optical interface circuit pack
- a defective local optical interface circuit pack

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action

1 If an Rx alarm occurs on G2, follow the procedure to clear the Fac DS1 STS1 path Rx CV, ES, SES, UAS threshold 1, 2 alarm. See page 4-29 for directions.

If the alarm	Then
clears	end the procedure.
persists	go to step 2.

2 If there is an Rx alarm on G1, follow the procedure to clear the Fac DS1 STS1 path Rx CV, ES, SES, UAS threshold 1, 2 alarm. See page 4-29 for directions.

If the alarm	Then
clears	end the procedure.
persists	contact your next level of support.

—end—

Fac DS3
STS1 Rx path trace failure

Probable cause

The system detected an error in the path trace information which accompanies each STS1 frame. One of the following reasons could cause this alarm:

- the upstream (transmitting) DS3/STS mapper is defective
- the upstream (transmitting) OC-3/OC-12 is defective
- the local OC-3/OC-12 is defective
- the local DS3/STS mapper is defective

If more than one STS1 path trace failure alarm is present at a network element, then a defective OC-3/OC-12 optical interface is likely the cause.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	From any network element FWPUI screen, display a list of active alarms and check for an OC-3/OC-12 equipment or facility alarm: **alarms**↵ *A summary list of alarms appears.*

If	Then
there is an OC-3/OC-12 alarm	go to step 3.
is no OC-3/OC-12 alarm	go to step 2.

Step	Action
2	Log in to the user interface at the upstream network element, display a list of active alarms, and check for an OC-3/OC-12 equipment or facility alarm.

If	Then
there is an OC-3/OC-12 alarm	go to step 3.
is no OC-3/OC-12 alarm	go to step 4.

—continued—

Fac DS3
STS1 Rx path trace failure (continued)

Step	Action

3 Look up the alarm in this document and proceed as instructed.

4 Perform a protection switch on the upstream DS3:

a. Display the DS3 protection switching screen:

pr;dtlprot ds3↵

The detailed protection screen appears.

b. Operate the manual switch:

manual op <group>↵
y↵

where

<group> DS3 circuit pack group from which traffic is being switched: see “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.

*The screen displays an asterisk * in the* `Manual` *column.*

If this alarm	Then
clears	go to step 7.
persists	go to step 5.

5 Perform a protection switch on the local DS3:

a. Log in to the local network element and display the DS3 protection switching screen:

pr;dtlprot ds3↵

The detailed protection screen appears.

b. Operate the manual switch:

manual op <group>↵
y↵

where

<group> is the DS3 circuit pack group from which traffic is being switched: see “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.

*The screen displays an asterisk * in the* `Manual` *column.*

If this alarm	Then
clears	go to step 7.
persists	go to step 6.

—continued—

Fac DS3
STS1 Rx path trace failure (continued)

Step	Action

6 Perform a protection switch on the local (receiving) OC-3/OC12:

a. Log in to the local network element and display the OC-3/OC-12 protection switching screen:

pr;dtlprot <type>

where

<type> is the type of optical circuit pack: **oc3** or **oc12**.

The detailed protection screen appears.

b. Operate the manual switch:

manual op <group>↵
y↵

where

<group> is the OC-3/OC-12 circuit pack group from which traffic is being switched: **g1** or **g2**.

*The screen displays an asterisk * in the* `Manual` *column.*

If this alarm	Then
clears	go to step 7.
persists	go to step 8.

7 Replace the circuit pack from which service was switched, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

8 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
STS1 Rx RFI

Probable cause

There is an alarm condition at the downstream (receiving) facility.
Any of the following conditions can cause this alarm:

- The local DS3/STS mapper is transmitting an invalid or alarmed STS1 signal.
- The local OC-3/OC-12 optical interface is transmitting an invalid or alarmed STS1 signal.
- The downstream (receiving) DS3/STS mapper is not properly receiving the STS1 signal.
- The downstream OC-3/OC-12 optical interface is not properly receiving the STS1 signal.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Clear the DS3 or OC-3/OC-12 equipment or facility alarm at the downstream (receiving) network element.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
STS1 Rx unequipped

Probable cause

The local DS3/STS mapper is not receiving an STS1 payload for one of the following reasons:

- all upstream DS3/STS1 facilities are out of service (OOS)
- the upstream DS3/STS mapper is defective

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action

1 Log in to the upstream network element user interface and display the DS3 facility screen to determine the state of the STS-1:

fa ds3 <group> <port>↵

where

<group>	is the group associated with STS1 alarm: see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15.
<port>	is the port number of the facility: **1** to **3**.

The DS3 facility screen appears. The STS1 state is the same as the facility state.

If the DS3 (STS1) state is	Then
OOS	go to step 2.
IS	go to step 3.

2 Change the DS3 facility state to in-service (IS):

chgstate is↵

The state of the DS3 (STS1) facility changes to in-service.

If this alarm	Then
clears	end the procedure.
persists	go to step 3.

—continued—

Fac DS3
STS1 Rx unequipped (continued)

Step	Action
3	Replace the upstream DS3/STS mapper, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
STS1 signal label mismatch

Probable cause

The terminations at the ends of an STS1 connection between two network elements are incompatible. For example, a DS1 on one network element is connected to a DS3 on another network element.

This alarm is raised at both ends of the connection.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	From the Connection Manager, verify the intended DS1-to-DS1 or DS3-to-DS3 connections set up. The alarm was raised because these connections are misaligned.
2	Replace either the DS3/STS mapper circuit pack or the DS1/VT mapper circuit pack at one end of the connection, as indicated in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
3	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
Tx AIS

Probable cause

An AIS signal from the fiber optics side of the DS3 has been received. The AIS was transmitted over the fiber from the DS3 at the far end.

Impact

This is a warning, service-affecting (w, SA) alarm.

Note: This is a secondary alarm. The primary alarm should be cleared.

Action

Step	Action
1	List the alarms, and check the DS3 facility and equipment at the far end for any failures: **alarms** ↵
2	If the far end facility has a DS3 Rx AIS, this is the cause of the DS3 Tx AIS alarm. Solve any problems indicated at the far end.
3	If the alarm is still not cleared, perform a DS3 protection switch at the far end NE. **pr** ↵ **dtlprot ds3** ↵ **manual op <group>** ↵ where <group> is the group number of the DS3: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.
4	If the alarm clears, replace the DS3/STS mapper at the far end. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.
5	Release the protection switch.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac DS3
Tx loss of frame

Probable cause

Framing has been corrupted on the DS3 signal across the fiber optics, or the DS3 signal coming from the far-end terminal is faulty.

Impact

This is a major, service-affecting (M, SA) alarm.

Note: This is a secondary alarm. The primary alarm should be cleared.

Action

Step	Action
1	List the alarms and check the DS3 facility and equipment for any failures: **alarms** ↵
2	If no relevant alarm is found, check the DS3 facility and equipment at the far end for any failures.
3	If the alarm is still not cleared, perform a DS3 protection switch at the far end NE. **pr** ↵ **dtlprot ds3** ↵ **manual op <group>** ↵ where <group> is the group number of the DS3: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.
4	If the alarm is cleared, proceed with the following, otherwise go to step 5. Replace the DS3/STS mapper at the far end. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.
5	Release the protection switch.

—continued—

Fac DS3
Tx loss of frame (continued)

Step	Action
6	Perform a DS3 protection switch at the local NE. **pr** ↵ **dtlprot ds3** ↵ **manual op <group>** ↵ where <group> is the group number of the DS3: See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.
7	If the alarm is cleared, proceed with the following, otherwise, go to step 9. Replace the DS3/STS mapper. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.
8	Release the switch.
9	Check the DS3 equipment (multiplexers and cross-connects) that is feeding the DS3 signal at the far end NE for faulty DS3 output or an incorrect LBO setting causing a weak signal. If faulty signals are found, take corrective action for the equipment involved.
10	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Fac DSX1
Facility loopback
Rx AIS
Rx babbling
Rx bipolar violation > 10E-3
Rx bipolar violation > 10E-4
Rx loss of frame
Rx loss of signal
Rx yellow
Terminal loopback

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543 for information on the following AccessNode Express alarms and the appropriate alarm clearing procedures.

These alarms are AccessNode Express DSX1 facility alarms.

—end—

Fac ESI
Bipolar violation

Probable Cause

A severe bipolar violation condition has been detected on the associated timing reference signal coming into the ESI.

Impact

This is a minor, service-affecting (m, SA) alarm if the secondary timing reference source is absent.

This is a minor, not service-affecting (m, nsa) alarm if the secondary timing reference source is present.

Action

Verify the primary and secondary reference connections to the central office's building integrated timing source (BITS) and verify the integrity of the timing reference sources (BITSA and BITSB).

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac ESI
Degraded clock carrier

Probable Cause

The external synchronization interface could not synchronize to the associated timing reference. This indicates an ESI circuit pack failure, or one of the following problems with the associated timing reference:

- the reference frequency is outside the Stratum 3 range
- there are excessive phase transients (amplitude or rate) on the associated reference

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Verify the integrity of the associated timing reference source. If the timing reference is within the Stratum 3 range, replace the ESI circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac ESI
Degraded timing reference

Probable cause

The ESI cannot synchronize to the incoming timing reference input signal.

The accuracy of the affected timing reference is lower than the accuracy of the internal clock. The accuracy of a reference is determined either by the provisioned value or from the S1 byte in the SONET overhead.

Impact

In an unprotected configuration, this is a major service-affecting (M, SA) alarm.

In a protected configuration, this is a minor not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Display the provisioning reference screen and verify provisioning.
2	If the provisioning is correct, call Nortel Networks support.

—end—

Fac ESI
Loss of frame

Probable Cause

A loss of frame has been detected on the associated timing reference.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	From the Network Element Status screen, display the ESI facility screen. **fa esi<timing reference>**↵ where <timing reference> is **bitsa** or **bitsb** *The ESI facility screen appears.*
2	Verify that the frame format of the timing reference input is equivalent to what is expected: **query all**↵ *The screen displays the current ESI facility parameters for the BITSA and BITSB timing reference.*

If the frame format	Then
is correct	go to step 3
is incorrect	a. Correct the frame format for the timing reference using the procedure for provisioning external synchronization parameters in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B. b. Determine if the alarm clears. If it clears, then end the procedure. If it persists, go to step 3.

—continued—

Fac ESI
Loss of frame (continued)

Step	Action
3	Check the connections of the external synchronization cable. ***Note:*** ESI connections should be checked at the timing reference (BITS) and at the appropriate jack on the side interconnect card of the common-equipment shelf. For details, see the procedure for installing an external synchronization cable in the Installation volume.

If the alarm	Then
clears	end the procedure.
persists	go to step 4.

4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac ESI
Loss of signal

Probable Cause

A loss of signal has been detected on the timing reference signal, either BITSA or BITSB. This alarm masks the “Fac ESI Loss of frame” alarm.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action

1 Check the connections of the external synchronization cable.

Note: ESI connections should be checked at the timing reference (BITS) and at the appropriate jack on the side interconnect card of the common-equipment shelf. For details, see the procedure for installing an external synchronization cable in the appropriate installation volume.

If the alarm	Then
clears	end the procedure.
persists	go to step 2.

2 From the Network Element Status screen, display the ESI facility screen.

fa esi <timing reference>↵

where

<timing reference> is **bitsa** or **bits**b.

The ESI facility screen appears.

—continued—

Fac ESI
Loss of signal (continued)

Step	Action
3	Verify that the frame format and line coding of the timing reference input is equivalent to what is expected: **query all**↵ *The screen displays the current ESI facility parameters for the BITSA and BITSB timing reference.*

If the frame format and line coding	Then
are correct	go to step 4.
are incorrect	a. Correct the frame format and line coding for the timing reference using the procedure for provisioning external synchronization parameters in *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B. b. Determine if the alarm clears. If it clears, then end the procedure. If it persists, go to step 4.

4	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac ESI
Oscillating sync status message

Probable cause

The incoming synchronization status message is oscillating.

Impact

In an unprotected configuration, this is a major service-affecting (M, SA) alarm.

In a protected configuration, this is a minor not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Display the provisioning reference screen and verify provisioning.
2	If the provisioning is correct, call Nortel Networks support.

—end—

Fac ESI
Reference forced switch request

Probable cause

A forced switch request was requested for synchronization references.

Impact

This is a minor, not service-affecting (m, nsa) alarm for information only.

Action

None.

—end—

Fac ESI
Reference manual switch request

Probable cause

A manual switch was requested for synchronization references.

Impact

This is a minor, not service-affecting (m, nsa) alarm for information only.

Action

None.

—end—

Fac ESI
Reference switch complete

Probable cause

Synchronization timing was successfully switched from one timing reference to another.

Impact

This is a warning, not service-affecting (w, nsa) alarm for information only.

Action

None.

—end—

Fac ESI
Reference switch fail

Probable cause

A requested protection switch from one synchronization reference to another failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Verify the integrity of the associated timing reference.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac ESI
Rx AIS

Probable cause

An alarm indication signal (AIS) has been detected on the timing reference.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Verify the integrity of the associated timing reference.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac ESI
Timing reference interface fail

Probable cause

One of the following conditions exists:

- loss of frame (LOF)
- loss of signal (LOS)
- frequency deviation

Impact

In an unprotected configuration, this is a major service-affecting (M, SA) alarm.
In a protected configuration, this is a minor not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Verify any alarms against ESI.
2	Clear the alarms according to the appropriate alarm clearing procedures in this document.
3	If the alarm persists, verify that the ESI facility is in service.
4	Verify that the timing reference input frame format is equivalent to what is expected by entering: **fac esi <timing reference>** ↵ where <**timing reference**> is **bitsa** or **bitsb**. **query all** ↵

If the frame format	**Then** go to
is not as expected	step 5.
is as expected	step 6.

5	Change the frame format. See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning,* Volume 4B.
6	Verify the connection of the external synchronization cable and the external reference signal.
7	If the alarm persists, contact Nortel Networks support for further assistance.

—end—

Fac ESI
Tx AIS

Probable cause

This alarm can be raised under the following conditions:

- The external synchronization interface circuit pack has lost signal reference from the optical carrier used by the ESI to generate a DS1 timing reference output.
- The S1 byte synchronization status message in the OC-n line, that is being used as a reference for the alarmed DS1 timing reference output, is at or below a user selectable quality level.
- An intercard alarm in the optical circuit pack group can cause the ESI timing reference output to generate an AIS signal.

  Note: This alarm may be generated when the OCA/OCB Timing Source provisioning is changed on the Trefsrc screen in which case the alarm will clear 10 seconds after it is raised.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Note: Verify that the relevant equipment and facilities are in service and active. No action is required if the relevant equipment is inactive.

Step	Action
1	To find which optic is relevant, query the affected timing reference output by entering: **fa esi <timing reference>** ↵ where **<timing reference>** is **g1out** or **g2out**. The relevant optic is the one which is used as the source for the ESI timing reference output. Verify that the input optical signal of the OC-3/OC-12 card is correct and that there are no active alarms for the OC-3/OC-12 facilities. If some alarms are present, correct them. Otherwise, go to step 2. **—continued—**

Fac ESI
Tx AIS (continued)

Step	Action
2	From the network element status screen, display the relevant equipment screen and verify that the state is IS (in service) by entering: **eq <service type> <circuit pack>** ↵ where **<service type>** is **oc3** or **oc12**. **<circuit pack group>** is **g1** or **g2**. *The equipment screen appears.* If the state is IS, go to step 4. If the status is standby, this is normal. If the equipment is not in service (IS), go to step 3.
3	Change the state to in service by entering: **chgstate is** ↵ *The state changes to IS.*
4	Display the list of active alarms and verify that the ESI alarm is cleared by entering: **alarms** ↵ *A list of active alarms appears.* If the ESI alarm is still present, go to step 5. If the alarm is cleared, stop here.
5	Display the relevant facility screen and verify that the state is IS (in service) by entering: **fa <service type> <circuit pack>** ↵ where **<service type>** is **oc3** or **oc12**. **<circuit pack>** is **g1** or **g2**. *The facility screen appears.* If the state is IS (in service) and the status is active, go to step 7. If the state is not IS (in service), go to step 6.

—continued—

Fac ESI
Tx AIS (continued)

Step	Action
6	Change the state of the facility to in service by entering: **chgstate is** ↵ *The state changes to IS (in service).*
7	The problem may be that the S1 byte synchronization status message in the OC-n line, that is being used as a reference for the alarmed DS1 timing reference output, is at or below a user selectable quality level. To view the user selectable quality level, enter: **fa esi <timing reference>** ↵ where **<timing reference>** is **g1out** or **g2out**. *The Threshold AIS field indicates the user selectable quality level.*
8	Determine if the far-end equipment connected to the OC-n line is sending a quality level in the S1 byte which is at or below the user selectable quality level.
9	If the problem persists, replace the ESI circuit pack carrying the ESI facility reporting the alarm (i.e., ESI G1 for G1OUT and ESI G2 for G2OUT). Refer to *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement.
10	Display the list of active alarms and verify that the ESI alarm is cleared by entering: **alarms** ↵ *A list of active alarms appears.*

If	Then
the ESI alarm is cleared	you have completed the procedure.
the ESI alarm is not cleared	call your next level of support.

—end—

Fac ESI
Undefined sync status message

Probable cause

The sync status message is not within the set of the defined values.

Impact

In an unprotected configuration, this is a major service-affecting (M, SA) alarm.

In a protected configuration, this is a minor not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Check the provisioned value for the sync message on that node and correct it if required.
2	If the problem persists, call Nortel Networks support.

—end—

Fac HDSL
ES threshold exceeded
Loopback
Loss of Sync
Margin threshold exceeded

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543 for information on the following AccessNode Express alarms and the appropriate alarm clearing procedures.

The following alarms are AccessNode Express HDSL facility alarms.

- HDSL errored seconds (ES threshold exceeded)
- HDSL loopback active (Loopback)
- HDSL loss of synchronization (Loss of Sync)
- HDSL margin (Margin threshold exceeded)

—end—

Fac OC-12
Inter-ring both feeds fail

Probable cause

This alarm indicates that the Service Selector on the Primary gateway in add-ring is not receiving any of the feeds (Primary as well as Secondary). Probable causes are:

- Facility or equipment provisioning problem at the service access point.
- Primary gateway node in Drop Ring is isolated and a failure is present on the secondary feed.

Impact

This is a critical, service-affecting (C, SA) alarm.

Note: This alarm indicates a loss of traffic.

Action

Step	Action
1	Check for Facility and Equipment provisioning problems at the source point.
2	Clear the alarms in the order of severity using the standard alarm clearing procedures.

—end—

Fac OC-12
Inter-ring forced switch request

Probable cause

This alarm is raised whenever a request for a forced switch on a primary gateway service selector.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

No action is necessary.

—end—

Fac OC-12
Inter-ring protection switch complete

Probable cause

This alarm is raised when the secondary feed is selected in the place of a primary feed (by a user initiated forced switch request or by a auto-switch request).

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Release the forced switch or the auto switch.

—end—

Fac OC-12
RX inter-ring secondary feed fail

Probable cause

This alarm indicates that the Service Selector on the Primary gateway in add-ring is not receiving Secondary feed. Probable causes are:

- Intra-ring switch in either the Drop (upstream), the Add Ring, or the Immediate Ring (only for DCP).
- STS channel fail alarm.
- Line AIS alarm or Path AIS alarm.
- Equipment alarms on the Primary and Secondary gateway nodes.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Check if the inter-ring both feed fail alarm is raised.
2	Clear the alarms in the order of severity using the standard alarm clearing procedures.
3	Check if the protection scheme is DCP, using the SSQUERY CI tool / OPC Connection Manager.
4	If the protection scheme is DCP, check for the intra-ring protection switch in both the adjacent rings.
5	Clear the fault causing the protection switch.

—end—

Fac OC-12
TX loss of inter-ring secondary feed

Probable cause

This alarm indicates that the Primary gateway in the drop-ring is not able to provide Secondary feed due to the intra-ring switch in the current ring. (DCP only.)

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

This alarm will automatically clear as soon as the intra-ring switch clears.

—end—

Fac OC-3/OC-12
Laser bias current

Probable cause

The laser bias current is no longer within the operating range required to maintain the laser output.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Note: If the alarm points have not been provisioned and activated, these alarm points show up as performance alerts.

Action

Step	Action

1 If the problem persists or worsens, replace the optical interface circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If the alarm	Then
clears	you have completed this procedure.
persists	go to step 2.

2 Increase the facility performance threshold value. See *Performance Monitoring Procedures*, 323-3001-520, in *Maintenance*, Volume 5C.

If the alarm	Then
clears	you have completed this procedure.
persists	contact your next level of support.

—end—

Fac OC-3/OC-12 **Line RFI**

Probable cause

The node issuing the remote failure indication (RFI) received a remote defect indication (RDI) from the far-end node the originates the STS1 line signal. The remote node issued the RDI because it received an STS1 loss of signal (LOS), STS1 loss of frame (LOF), or STS1 line alarm indication signal (AIS).

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	Check the node where the STS1 line signal originates for STS1 LOS, STS1 LOF, or STS1 line AIS alarms.
2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac OC-3/OC-12
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2
Line Rx UAS threshold 1, 2
Sect Rx CV threshold 1, 2
Sect Rx ES threshold 1, 2
Sect Rx SES threshold 1, 2
Sect Rx SEFS threshold 1, 2

Probable cause

For Line Rx CV: the number of code violations (CV) detected in the SONET line overhead has exceeded a threshold setting.

For Line Rx ES: the number of errored seconds (ES) detected in the SONET line overhead has exceeded a threshold setting.

For Line Rx SES: the number of severely errored seconds (SES) detected in the SONET line overhead has exceeded a threshold setting.

For Line Rx UAS: the number of one second intervals during which the SONET line is unavailable.

For Sect Rx CV: the number of code violations (CV) detected in the SONET section overhead has exceeded a threshold setting.

For Sect Rx ES: the number of errored seconds (ES) detected in the SONET section overhead has exceeded a threshold setting.

For Sect Rx SES: the number of severely errored seconds (SES) detected in the SONET section overhead has exceeded a threshold setting.

For Sect Rx SEFS: the number of errored frame seconds SEFS detected in the SONET section overhead has exceeded a threshold setting.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

—continued—

Fac OC-3/OC-12
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2
Line Rx UAS threshold 1, 2
Sect Rx CV threshold 1, 2
Sect Rx ES threshold 1, 2
Sect Rx SES threshold 1, 2
Sect Rx SEFS threshold 1, 2 (continued)

Action

Clear this alarm using following procedure.

Step	Action
1	From the network element status screen display the OC-3/OC-12 facility performance statistics screen: **pm;facperf <type> < group >↵** **If you have this <type> of optical circuit pack** / **Then your <group> number is** OC-3 / all, g1, g2, g1s, g2s, g3, g4, g5, g6, g7, or g8 OC-12 / all, g1, or g2 *The facility performance statistics screen appears.*
2	Display the history for this alert: **history <alert>↵** where <alert> is the alert for which historical information is required: **sectcv, sectes, sectses, sectsefs, linecv**, **linees**, **lineses, lineuas,** or **linefc**. *The performance history screen appears.*

If the counts are	Then
intermittent	go to step 3.
occurring regularly	go to step 4.

—continued—

Fac OC-3/OC-12
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2
Line Rx UAS threshold 1, 2
Sect Rx CV threshold 1, 2
Sect Rx ES threshold 1, 2
Sect Rx SES threshold 1, 2
Sect Rx SEFS threshold 1, 2 (continued)

Step	Action

3 Monitor the performance counts:

If the counts	Then
do not increase	the problem has cleared.
increase or become more regular	go to step 4.

4 Display the OC-3/OC-12 protection switching screen:

pr;dtlprot <type>↵

where

<type> is the type of optical circuit pack: **oc3** or **oc12**.

The OC-12 protection switching screen appears.

5 Switch traffic to the protection (standby) OC-3/OC-12 optical interface:

forced op < group >↵

If you have this type of optical circuit pack	Then your group number is
OC-3	all, g1, g2, g1s, g2s, g3, g4, g5, g6, g7, or g8
OC-12	all, g1, or g2

CAUTION
Risk of circuit pack damage
Wear a properly grounded antistatic wrist strap to avoid damage to equipment.

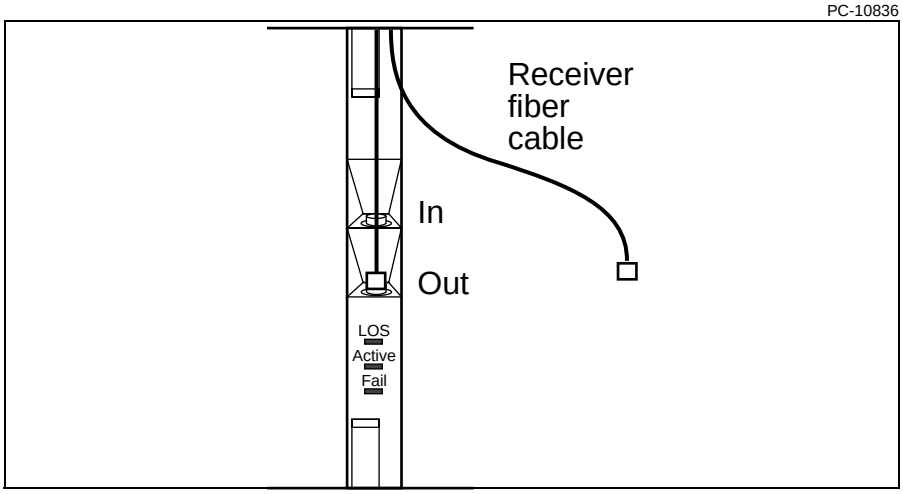
DANGER
Risk of personal injury
Avoid direct exposure to laser beam or fiber.

—continued—

Fac OC-3/OC-12
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2
Line Rx UAS threshold 1, 2
Sect Rx CV threshold 1, 2
Sect Rx ES threshold 1, 2
Sect Rx SES threshold 1, 2
Sect Rx SEFS threshold 1, 2 (continued)

Step	Action
6	Disconnect the receiver fiber cable from the Rx connector on the suspect optical interface (this is the optical interface that is no longer carrying traffic).

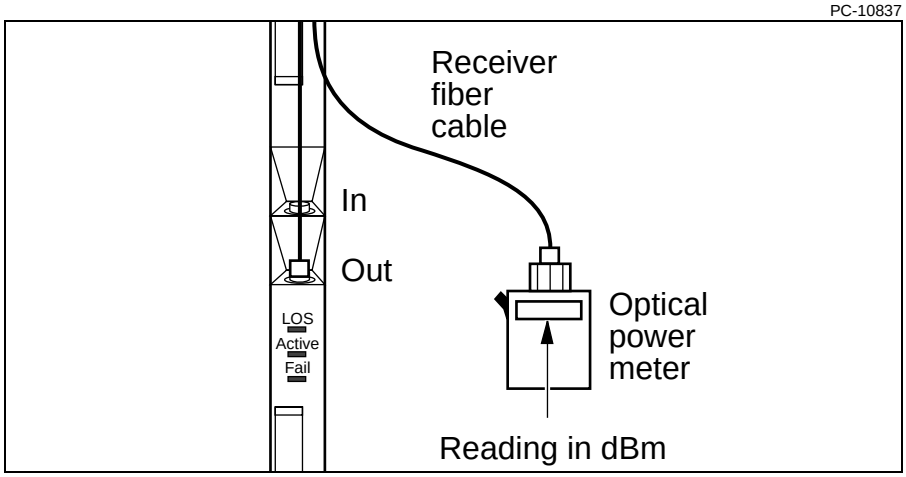
PC-10836



7	Clean the optical connectors by carefully blowing inside the connectors with compressed air.

—continued—

Fac OC-3/OC-12
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2
Line Rx UAS threshold 1, 2
Sect Rx CV threshold 1, 2
Sect Rx ES threshold 1, 2
Sect Rx SES threshold 1, 2
Sect Rx SEFS threshold 1, 2 (continued)

Step	Action
8	Connect the receiver fiber cable to an optical power meter and measure the receiver optical power level: For long reach OC-3 (NT7E01CA, CB, CC or CD): measure for a level greater than or equal to –34.0 dBm (for example –32.0 dBm). For intermediate reach OC-3 (NT7E01DA, DB, DC or DD) measure for a level greater than or equal to –28.0 dBm (for example –26.0 dBm). For long reach OC-12 (NT7E02KA, KB, KC, or KD): measure for a level greater than or equal to –32.0 dBm (for example –28.0 dBm). For intermediate reach OC-12 (NT7E02LA, LB, LC, or LD) measure for a level greater than or equal to –24.5 dBm (for example –23.0 dBm). PC-10837 

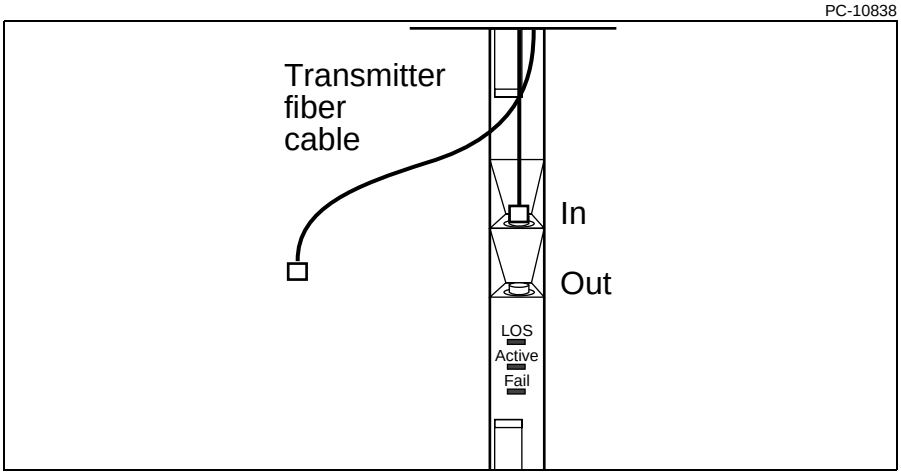
If the signal level is	Then
correct	go to step 14.
incorrect	go to step 9.

—continued—

Fac OC-3/OC-12
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2
Line Rx UAS threshold 1, 2
Sect Rx CV threshold 1, 2
Sect Rx ES threshold 1, 2
Sect Rx SES threshold 1, 2
Sect Rx SEFS threshold 1, 2 (continued)

Step	Action
9	At the far-end optical interface that is not carrying traffic, disconnect the transmitter fiber cable from the Tx connector on the circuit pack.

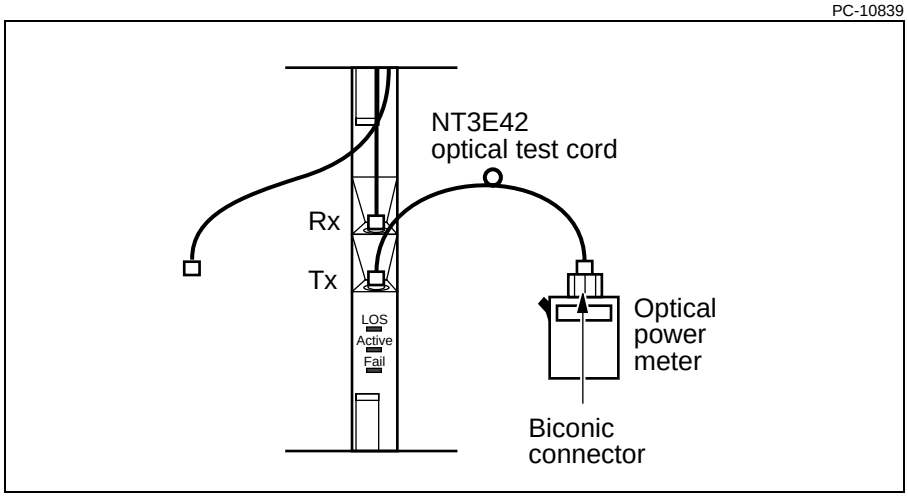
PC-10838



10	Clean the optical connectors by blowing inside the connectors with compressed air.

—continued—

Fac OC-3/OC-12
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2
Line Rx UAS threshold 1, 2
Sect Rx CV threshold 1, 2
Sect Rx ES threshold 1, 2
Sect Rx SES threshold 1, 2
Sect Rx SEFS threshold 1, 2 (continued)

Step	Action
11	Connect one end of the optical test cord to the optical power meter through the 2017 biconic adapter, and connect the other end to the transmitter optical connector on the circuit pack. Measure the transmit optical level. For long reach OC-3 (NT7E01CA, CB, CC or CD): measure for a level greater than or equal to –5.0 dBm (for example –2.5 dBm). For intermediate reach OC-3 (NT7E01DA, DB, DC or DD) measure for a level greater than or equal to –15.0 dBm (for example –14.0 dBm). For long reach OC-12 (NT7E02KA, KB, KC, or KD): measure for a level greater than or equal to –3.0 dBm (for example –2.5 dBm). For intermediate reach OC-12 (NT7E02LA, LB, LC, or LD) measure for a level greater than or equal to –4.5 dBm (for example –4.0 dBm). PC-10839 

If the signal level is	Then
correct	go to step 12.
incorrect	go to step 14.

—continued—

Fac OC-3/OC-12
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2
Line Rx UAS threshold 1, 2
Sect Rx CV threshold 1, 2
Sect Rx ES threshold 1, 2
Sect Rx SES threshold 1, 2
Sect Rx SEFS threshold 1, 2 (continued)

Step	Action
12	If there is no miniature variable optical attenuator skip this step. Adjust the miniature variable optical attenuator to achieve the correct signal level. If the level is met end here. If the level cannot be met, go to next step.
13	The problem is with the optical fiber cable. Report this condition to outside plant maintenance, and end the procedure.
14	Replace the optical interface, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
15	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac OC-3/OC-12 **Loss of frame**

Probable cause

An OC-12 frame can no longer be detected on the optical fiber coming to the equipment due to one of the following reasons.

- signal degradation (degraded fiber or transmitter failure)
- the received optical power is low
- the connector of the receiver unit is dirty
- the miniature variable optical attenuator (mVOA) is malfunctioning
- the fiber optics patchcord is damaged
- the receiver unit is defective

Impact

This is a critical, service-affecting (C, SA) alarm, (if not protectable).
This is a minor, not service-affecting (m, nsa) alarm, (if protectable).
Upon detection of the failure, a high-speed switch occurred and caused a traffic outage of no more than 60 ms.

Action

Isolate the fault by measuring optical power at the optical receiver and the transmitter, by performing the following steps.

Step	Action
1	The fiber connected to the OC-12 optics in alarm must be removed in order to be checked. However, before unplugging the module, ensure that live traffic is being received by the other OC-12 optics. If the circuit in alarm is the working OC-12 optical interface circuit pack, go to step 2. Otherwise, go to step 3. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for removal and insertion of the OC-12 optics.

—continued—

Fac OC-3/OC-12
Loss of frame (continued)

Step	Action
2	Ensure that there is no lockout by entering: **protectn** ↵ **dtlprot <type> [<unit>]**↵ where **<type>** is **oc12**. **<unit>** is **g1** or **g2**. ***Note*:** The <unit> parameter is not required for OC-12 terminals or ring ADMs. If a lockout is in effect, that is, next to the lockout field either an * or an *R is present, the lockout must be removed. If * is found, enter: **lockout re** ↵ **yes** ↵ For ring nodes, enter: **lockout re w** ↵ **yes** ↵ *or* **lockout re p** ↵ **yes** ↵ If *R is found, the lockout must be deactivated at the remote end. Login to the remote end and enter: **lockout re** ↵ **yes** ↵ For ring nodes, enter: **lockout re w** ↵ **yes** ↵ *or* **lockout re p** ↵ **yes** ↵
3	Force the live traffic to the other OC-3/OC-12 optics by entering: **forced op <unit>** ↵ **yes**↵ where <unit> can be **g1, g2, g2s, g1s, g3** to **g8**.

—continued—

Fac OC-3/OC-12
Loss of frame (continued)

Step	Action
4	Unplug the fiber connected to the receive In connector (top) of the OC-12 optics in alarm which is deprived of traffic, and clean the optical connector as outlined in *Commissioning and Testing,* Volume 3.
5	Measure the received optical power using an optical power meter. The received power should be as shown in the table below. If the received power is not within this range, adjust the mVOA if equipped until it is.

Optical interface circuit pack	**Received power**	
	minimum (dBm)	**maximum (dBm)**
OC-12 IR (NT7E02)	–24.5	–4.0
OC-12 LR (NT7E02)	–32.0	–7.0
OC-12 VTBM IR (NT7E05)	–28.0	–8.0
OC-12 VTBM LR (NT7E05)	–29.5	–8.0
Note: The above requirements for OC-12 VTBM units are for an NT-to-NT proprietary link. For a link meeting the Bellcore Midspan meet specification, the following requirements apply:		
OC-12 VTBM IR (NT7E05)	–28.0	–8.0
OC-12 VTBM LR (NT7E05)	–29.5	–8.0

6	If the received power cannot be adjusted to be within the specification boundaries, measure the receiving power before the mVOA (for example, at the fiber patch panel).
7	If the power before the mVOA is low, go to step 9. Otherwise, go to step 8.
8	The fiber patchcord is faulty. Try another patchcord equipped with an mVOA having the same attenuation range. Make sure not to bend the fiber more than what the fiber manufacturer specifies (no more than 76 mm [3 in.] bending radius). The yellow LOS (loss of signal) LED should then turn OFF. If the LED remains ON, go to step 9.
9	Move to the upstream site. At the new location, using a patchcord without mVOA, measure the transmitted power.

—continued—

Fac OC-3/OC-12
Loss of frame (continued)

Step	Action

10 If the transmit power is within the specified limits, then go to step 11. If the transmit power is not within the specified limits, replace the OC-12 optical interface circuit pack.See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

Optical interface circuit pack	**Transmit power**	
	minimum (dBm)	**maximum (dBm)**
OC-12 IR (NT7E02)	–4.5	+1.5
OC-12 LR (NT7E02)	–3.0	+2.0
OC-12 VTBM IR (NT7E05)	–15.0	–8.0
OC-12 VTBM LR (NT7E05)	–1.5	+2.0
Note: The above requirements for OC-12 VTBM units are for an NT-to-NT proprietary link. For a link meeting the Bellcore Midspan meet specification, the following requirements apply:		
OC-12 VTBM IR (NT7E05)	–15.0	–8.0
OC-12 VTBM LR (NT7E05)	–1.5	+2.0

11 If the problem persists, replace the OC-12 optical interface circuit pack reporting the alarm. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

12 If the problem persists, replace the OC-12 optical interface circuit pack at the far-end network element which is connected to the circuit pack reporting the alarm. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

13 Release the forced switch done previously in step 3 by typing:

protectn ↵
dtlprot <type> [<unit>]↵
forced re ↵ (depending on where the switch was done)
yes ↵

where

<type> is **oc12**.

<unit> is **g1** or **g2**.
***Note*:** The <unit> parameter is not required for OC-12 terminals or ring ADMs.

—end—

Fac OC-3/OC-12 **Rx AIS**

Probable cause

There is an alarm condition at the up-stream (transmitting) OC-3 or OC-12 facility.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	Check the up-stream (transmitting) network element for OC-3 or OC-12 equipment or facility alarms.
2	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac OC-3/OC-12 **Rx loss of signal**

Probable cause

A signal can no longer be detected on the optical fiber coming into the equipment due to:

Note: An OC-3 loss of frame condition is reported as an OC-3 Rx loss of signal (LOS) alarm. See “Loss of frame” on page 4-135.

- fiber cut
- transmitter failure
- received optical power too low
- dirty receiver unit connector
- malfunctioning miniature variable optical attenuator (mVOA)
- damaged fiber optics patchcord
- defective receiver unit
- the rate receive signal does not match the optical interface circuit pack, for example an OC-3 signal is connected to an OC-12 circuit pack

Impact

This is a critical, service-affecting (C, SA) alarm, (if not protectable).
This is a minor, not service-affecting (m, nsa) alarm, (if protectable).
Upon detection of the failure, a high-speed switch occurred and caused a traffic outage of no more than 60 ms.

Action

Step	Action
1	The fiber connected to the OC-3/OC-12 optics in alarm must be removed in order to be checked. However, before unplugging the module, ensure that live traffic is being received by the other OC-3/OC-12 optics. If the circuit in alarm is the working OC-3/OC-12 optical interface circuit pack, go to step 2. Otherwise, go to step 3. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for removal and insertion of the OC-3/OC-12 optics. ***Note:*** If this alarm is seen for unprotected OC-3 tributaries, then this procedure cannot be performed in service since there is no OC-3 trib to switch to.

—continued—

Fac OC-3/OC-12
Rx loss of signal (continued)

Step	Action
2	Ensure that there is no lockout by entering: **protectn** ↵ **dtlprot <type> [<unit>]**↵ where **<type>** is **oc3** or **oc12**. **<unit>** is **g1** or **g2** (for OC-12 or OC-3 feeder) is **g3** to **g8**, **g1s**, or **g2s** (for OC-3 tributaries) ***Note*:** The <unit> parameter is not required for OC-12 terminals or ring ADMs. If a lockout is in effect, that is, next to the lockout field either an * or an *R is present, the lockout must be removed. If * is found, enter: **lockout re** ↵ **yes** ↵ For ring nodes, enter: **lockout re w** ↵ **yes** ↵ *or* **lockout re p** ↵ **yes** ↵ If *R is found, the lockout must be deactivated at the remote end. Login to the remote end and enter: **lockout re** ↵ **yes** ↵ For ring nodes, enter: **lockout re w** ↵ **yes** ↵ *or* **lockout re p** ↵ **yes** ↵
3	Force the live traffic to the other OC-3/OC-12 optics by entering: **forced op <unit>** ↵ **yes**↵ where <unit> can be **g1, g2, g2s, g1s, g3** to **g8**.

—continued—

Fac OC-3/OC-12
Rx loss of signal (continued)

Step	Action

4 Unplug the fiber connected to the receive In connector (top) of the OC-3/OC-12 optics in alarm which is deprived of traffic, and clean the optical connector as outlined in *Commissioning and Testing,* Volume 3.

5 Measure the received optical power using an optical power meter. The received power should be as shown in the table below. If the received power is not within this range, adjust the mVOA if equipped until it is.

Optical interface circuit pack	**Received power**	
	minimum (dBm)	**maximum (dBm)**
OC-3 IR (NT7E01)	–28.0	–8.0
OC-3 LR (NT7E01)	–34.0	–10.0
OC-12 IR (NT7E02)	–24.5	–4.0
OC-12 LR (NT7E02)	–32.0	–7.0
OC-12 VTBM IR (NT7E05)	–28.0	–8.0
OC-12 VTBM LR (NT7E05)	–29.5	–8.0
Note: The above requirements for OC-12 VTM units are for an NT-to-NT proprietary link. For a link meeting the Bellcore Midspan meet specification, the following requirements apply:		
OC-12 VTBM IR (NT7E05)	–28.0	–8.0
OC-12 VTBM LR (NT7E05)	–29.5	–8.0

6 If the received power cannot be adjusted to be within the specification boundaries, measure the receiving power before the mVOA (for example, at the fiber patch panel).

7 If the power before the mVOA is low, go to step 9. Otherwise, go to step 8.

8 The fiber patchcord is faulty. Try another patchcord equipped with an mVOA having the same attenuation range. Make sure not to bend the fiber more than what the fiber manufacturer specifies (no more than 76 mm [3 in.] bending radius). The yellow LED should then turn OFF. If the LED remains ON, go to step 9.

9 Move to the upstream site. At the new location, using a patchcord without mVOA, measure the transmitted power.

—continued—

Fac OC-3/OC-12
Rx loss of signal (continued)

Step	Action

10 If the transmit power is within the specified limits, then go to step 11. If the transmit power is not within the specified limits, replace the OC-3/OC-12 optical interface circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

Optical interface circuit pack	**Transmit power**	
	minimum (dBm)	**maximum (dBm)**
OC-3 IR (TN7E01)	–15.0	–8.0
OC-3 LR (TN7E01)	–5.0	0.0
OC-12 IR (NT7E02)	–4.5	+1.5
OC-12 LR (NT7E02)	–3.0	+2.0
OC-12 VTBM IR (NT7E05)	–15.0	–8.0
OC-12 VTBM LR (NT7E05)	–1.5	+2.0
Note: The above requirements for OC-12 VTBM units are for an NT-to-NT proprietary link. For a link meeting the Bellcore Midspan meet specification, the following requirements apply:		
OC-12 VTBM IR (NT7E05)	–15.0	–8.0
OC-12 VTBM LR (NT7E05)	–1.5	+2.0

11 If the problem persists, replace the OC-3/OC-12 optical interface circuit pack reporting the alarm. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

12 If the problem persists, replace the OC-3/OC-12 optical interface circuit pack at the far-end network element which is connected to the circuit pack reporting the alarm. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

13 Release the forced switch done previously in step 3 by typing:
protectn ↵
dtlprot <type> [<unit>]↵
forced re ↵ (depending on where the switch was done)
yes ↵

where

<type> is **oc3** or **oc12**.

<unit> is **g1** or **g2** (for OC-12 or OC-3 feeder)
is **g3** to **g8**, **g1s**, or **g2s** (for OC-3 tributaries)
***Note*:** The <unit> parameter is not required for OC-12 terminals or ring ADMs.

—end—

Fac OC-3/OC-12
Section Rx optical power threshold

Probable cause

One of the following conditions causes this alarm:

- a defective fiber
- a fiber that is failing
- a dirty connector

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Note: In isolation this alarm does not affect service; however, it might appear with other alarms that are critical. In that circumstance, the critical alarms will affect service.

Action

Step	Action
1	Use an optical power meter to check the power levels on the optical fibers.
2	Complete the instructions in the following table:

If	Then
the power levels are correct	reinsert the fiber.
the power levels are incorrect	readjust the power levels.
the alarm persists	go to step 3.

Step	Action
3	Check the threshold provisioning screen and complete the instructions in the following table:

If the provisioned value is	Then
inappropriate	reprovision the value.
appropriate	call your Nortel Networks representative.

—end—

Fac OC-3/OC-12 **Signal degrade**

Probable cause

The local OC-3 or OC-12 optical interface is receiving a signal that is degraded beyond the signal degrade threshold (from 10^{-4} to 10^{-10}) due to one of the following reasons:

- far-end transmitter malfunction
- dirty receiver connector or malfunctioning mini-variable optical attenuator (MVOA)
- defective receiver on the OC-3 or OC-12 optical interface

Impact

In an unprotected configuration, this is a minor, service-affecting (m, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	Log in to the user interface at the far end network element, display a list of active alarms, and check for an OC-3/OC-12 alarm: **alarms** ↵ *A summary list of alarms appears.*

If	Then
there is an OC-3/OC-12 alarm	go to step 2.
there is no OC-3/OC-12 alarm	go to step 6.

2	Look up the alarm in this document and proceed accordingly.
3	If the circuit pack in alarm is the active OC-3/OC-12 optical interface circuit pack, go to step 4; otherwise go to step 6.

—continued—

Fac OC-3/OC-12
Signal degrade (continued)

Step	Action

4 Ensure there is no lockout by entering:

protectn ↵

dtlprot <type> ↵

where

<type> is the type of optical facility: **oc3** or **oc12**.

If a lockout is in effect, the lockout must be removed.

lockout re ↵

yes ↵

5 Force the traffic to the standby OC-3/OC-12 optics by entering:

forced op <group> ↵

yes ↵

If you have this type of optical circuit pack	Then your <group> number is
OC-3	all, g1, g2, g1s, g2s, g3, g4, g5, g6, g7, or g8.
OC-12	all, g1, or g2.

Go to step 6.

6 At the receive end where the signal degrade alarm is raised, unplug the fiber connected to the In port (top) of the OC-3/OC-12 optics in alarm which is deprived of traffic, and clean the optical connector as outlined in *Commissioning and Testing*, Volume 3.

Measure the received optical power using an optical power meter. The received power should be as shown in the table below. If the received power is not within this range, adjust the MVOA until it is.

Optical interface circuit pack	Received power	
	Minimum (dBm)	Maximum (dBm)
OC-12 IR	–24.5	–4.0
OC-12 LR	–32.0	–7.0
OC-3 IR	–28.0	–8.0
OC-3 LR	–34.0	–10.0

7 If the received power cannot be adjusted to be within the specification boundaries, measure the receiving power before the mVOA (for example, at the fiber cross-connect).

—continued—

Fac OC-3/OC-12
Signal degrade (continued)

Step	Action

8 If the power before the mVOA is low, go to step 10. Otherwise, go to step 9.

9 The fiber patchcord is faulty. Try another patchcord equipped with an mVOA having the same attenuation range. Make sure not to bend the fiber more than what the fiber manufacturer specifies (no more than 76 mm [3 inches] bending radius). The yellow LED should then turn OFF. If it remains ON, go to step 10.

10 At the far-end network element, measure the transmitted power.

If the transmitted power is within the specified limits (see table below), the problem resides in the fiber between the Transmitter and Receiver. If the transmit power is not within the specified limits, replace the active OC-3/OC-12 optical interface circuit pack. Refer to *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

Optical interface circuit pack	Transmit power minimum (dBm)
OC-12 IR	–4.5
OC-12 LR	–3.0
OC-3 IR	–15.0
OC-3 LR	–5.0

If a forced switch was activated (step 5), go to step 11.

If not, end the procedure.

11 Once done, release the forced switch and type the following:

forced re <group> ↵

yes ↵

If you have this type of optical circuit pack	Then your <group> number is
OC-3	all, g1, g2, g1s, g2s, g3, g4, g5, g6, g7, or g8.
OC-12	all, g1, or g2.

12 If the alarm persists, replace the OC-12 circuit pack where the failure is reported. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

13 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac OC3/OC12 **Signal fail**

Probable cause

The optical signal coming into the equipment has degraded beyond the signal fail threshold (from 10^{-3} to 10^{-5}).

- fiber cut
- transmitter failure
- received optical power too low
- dirty receiver unit connector
- malfunctioning mini-variable optical attenuator (mVOA)
- damaged fiber optics patchcord
- defective Receiver unit

Impact

This is a critical, service-affecting (C, SA) alarm (if not protectable).
This is a minor, not service-affecting (m, nsa) alarm (if protectable).
Upon detection of the failure, a high-speed switch occurred and caused a traffic outage of no more than 60 ms.

Action

Step	Action
1	The fiber connected to the OC-3/OC-12 optics in alarm must be removed in order to be checked. However, before unplugging the module, ensure that live traffic is being received by the other OC-3/OC-12 optics. If the circuit in alarm is the working OC-3/OC-12 optical interface circuit pack, go to step 2. Otherwise, go to step 3. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for removal and insertion of the OC-3/OC-12 optics. ***Note:*** If this alarm is seen for unprotected OC-3 tributaries, then this procedure cannot be performed in service since there is no OC-3 trib to switch to. **—continued—**

Fac OC3/OC12
Signal fail (continued)

Step	Action
2	Ensure that there is no lockout by entering: **protectn** ↵ **dtlprot <type> [<group>]**↵ where **<type>** is **oc3** or **oc12**. **<group>** is **g1** or **g2** (for terminal or VTBM ring ADM) is **g1** or **g1s** (for NWK ring ADM) is **g1, g2, g1s** or **g2s** (for linear ADM) is **g3** to **g8**, **g1s**, or **g2s** (for oc-3 tributaries) *Note*: The <unit> parameter is not required for oc-12 terminals or ring ADMs. If a lockout is in effect, that is, next to the lockout field either a * or a *R is present, the lockout must be removed. If * is found, enter: **lockout re** ↵ **yes** ↵ For ring ADMs, enter: **lockout re w** ↵ **yes** ↵ *or* **lockout re p** ↵ **yes** ↵ If *R is found, the lockout must be deactivated at the remote end. Login to the remote end and enter: **lockout re** ↵ **yes** ↵ For ring ADMs, enter: **lockout re w** ↵ **yes** ↵ *or* **lockout re p** ↵ **yes** ↵

—continued—

Fac OC3/OC12
Signal fail (continued)

Step	Action

3 Force the live traffic to the other OC-3/OC-12 optics by entering:

forced op <group> ↵
yes↵

where

<group> can be **g1, g2, g2s, g1s, g3** to **g8**.

4 Unplug the fiber from the alarmed optical interface circuit pack. Clean the fiber using the appropriate procedure for cleaning fiber optic connectors found in *Commissioning and Testing,* Volume 3.

5 Verify that the received optical power is in the correct range using the procedure found in *Data Administration Procedures,* 323-3001-304, in *Operations, Administration, and Provisioning*, Volume 4A.

Measure the received optical power using an optical power meter. The received power should be as shown in the table below. If the received power is not within this range, adjust the mVOA if equipped until it is.

Optical interface circuit pack	**Received power**	
	minimum (dBm)	**maximum (dBm)**
OC-3 IR (NT7E01)	–28.0	–8.0
OC-12 IR (NT7E02)	–24.5	–4.0
OC-12 ELR (NT7E02)	–32.2	–8.0
OC-12 VTBM IR (NT7E05)	–28.0	0
Note: The above requirements for OC-12 VTBM units are for an NT-to-NT proprietary link. For a link meeting the Bellcore Midspan meet specification, the following requirements apply:		
OC-12 VTBM IR (NT7E05)	–28.0	–8.0

6 If the received power cannot be adjusted to be within the specification boundaries using the mVOA, measure the received power at the origin in the network element location (in the fiber patch panel, for example).

7 If the measured power at the origin is within range, go to step 8. Otherwise, go to step 9.

8 The fiber patchcord is faulty. Try another patchcord with the same specifications. Make sure not to bend the fiber more than its bending radius of 76 mm (3 in.). Reconnect the fiber to the optical interface circuit pack. If problem is not solved, go to step 9.

—continued—

Fac OC3/OC12
Signal fail (continued)

Step	Action
9	Replace the optical interface circuit pack. Refer to *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.
10	Access the OC-3/OC-12 performance monitoring section parameters by entering: **perfmon** ↵ **facperf oc3** or **oc12 <circuit pack group>** ↵ where **<circuit pack group>** is the group number of the upstream optical interface **g1**, **g1s**, **g2**, or **g2s, g1e, g1w g3** to **g8**. Monitor this screen. Errors indicate that the problem has not been corrected. Go to step 11.
11	Replace the optical interface circuit pack at the far-end network element. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.
12	At the near-end network element, use the OC-3/OC-12 performance monitoring statistics screen to verify if the problem has been corrected.
13	Release the forced switch done previously in step 3 by typing: **protectn** ↵ **dtlprot <type> [<group>]**↵ where **<type>** is **oc3** or **oc12**. **<group>** is **g1** or **g2** (for terminal or VTBM ring ADM) is **g1** or **g1s** (for NWK ring ADM) is **g1, g2, g1s** or **g2s** (for linear ADM) is **g3** to **g8**, **g1s**, or **g2s** (for oc-3 tributaries) ***Note*:** The <group> parameter is not required for oc-12 terminals or ring ADMs. **forced re** ↵ (depending on where the switch was done) **yes** ↵
14	If the alarm persists, replace the OC-12 circuit pack where the failure is reported. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

—end—

Fac OC-3/OC-12 **STS1 Rx AIS**

Probable cause

An alarm condition exists at the upstream (transmitting) DS1, DS3, transport interface card (TIC), or OC-3/OC-12 facility.

In a universal (UDLC) configuration, the alarm condition is at the upstream (transmitting) OC-3/OC-12 or TIC.

In an integrated (IDLC) configuration, the alarm condition is at the upstream OC-3/OC-12 or DS1.

In a combined configuration, the alarm condition is at the upstream OC-3/OC-12, DS1, or TIC.

In an IDLC or DS1 tandem configuration, the alarm condition is at the upstream (transmitting) TIC.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Log in at the upstream (transmitting) network element user interface and display the list of active alarms by entering: **alarms**↵ *The system displays a list of alarms in decreasing order of severity.*
2	Check for other TIC, DS1, DS3, or OC-3/OC-12 alarms. ***Note 1:*** In a UDLC configuration, check for TIC or OC-3/OC-12 alarms at the upstream (transmitting) site. ***Note 2:*** In an IDLC or DS1 tandem configuration, check for OC-3/OC-12 or DS1 alarms at the upstream site. ***Note 3:*** In a combined configuration, check for OC-3/OC-12, DS1, or TIC alarms at the upstream site.

—continued—

Fac OC3/OC12
STS1 Rx AIS (continued)

Step	Action

If	Then
TIC alarms are displayed	go to step 4.
DS1, DS3, or OC-3/OC-12 alarms are displayed	go to step 7.
no DS1, DS3, TIC, or OC-3/OC-12 alarms are displayed	go to step 3.

3 Replace the local (receiving) DS1/VT mapper, DS3/STS mapper, or TIC circuit pack at the network element where the STS1 Rx AIS alarm was originally displayed. For details, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If the alarm	Then
clears	end the procedure.
persists	contact your next level of support.

4 To determine the upstream facility source of the TIC alarm, log in to the operations controller (OPC) and open the Connection Manager tool. See the procedure for logging in to the OPC and opening an OPC tool in *Data Administration Procedures,* 323-3001-304, in *Operations, Administration, and Provisioning*, Volume 4A.

If Connection Services have been enabled, the tool opens and displays tributary information. (If Connection Services have not been enabled, an informational dialog appears, and the tool closes.)

5 Find the STS-1 alarm in the right column of the Connection Manager and note the tributary information from both network elements for this STS.

6 From Table 4-11 on page 4-154, which lists STS default mapping, determine the mapping of the TIC STS-1 facilities, such as which STS-1 facilities are connected to the TIC (port 1 or 2 or both).

—continued—

Fac OC-3/OC-12
STS1 Rx AIS (continued)

Step Action

Table 4-11

Configuration	FCOT	RFT	STS#
UDLC	TIC STS-1 #2	TIC STS-1 #2	2
IDLC (ABM FCOT)	DS1 G1, G2	TIC STS-1 #1	1
IDLC (TBM FCOT)	DS1 G3, G4	TIC STS-1 #1	1
Combined: IDLC UDLC	 DS1 G1, G2 TIC STS-1 #2	 TIC STS-1 #1 TIC STS-1 #2	 1 2

7 Look up the alarms in this document and follow the procedures to clear them

If the STS1 Rx AIS alarm	Then
clears	end the procedure
persists	go to step 8

8 At the operations controller (OPC), enter the Connection Manager and check for alarms on intermediate nodes through which the STS connection passes. If you find equipment or facility alarms against the primary or secondary optics on the intermediate nodes, look up the alarms in this document and follow the procedures to clear them.

9 From the far-end network element user interface, manually switch the far end equipment.

If the STS1 Rx AIS alarm	Then
clears	replace the far-end equipment (see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C).
persists	go to step 10.

—continued—

Fac OC-3/OC-12
STS1 Rx AIS (continued)

Step	Action
10	From the local network element user interface, manually switch the DS1 or DS3 circuit pack by entering: **protectn**↵ **dtlprot <type>**↵ **manual op <circuit pack group>**↵ where **<type>** **ds1** or **ds3**. **<circuit pack group>** **g1** or **g2**.

If the STS1 Rx AIS alarm	Then
clears	replace the circuit pack (see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C)
persists	go to step 11

11	Release the manual switch by entering: **protectn**↵ **dtlprot <type>**↵ **manual re <circuit pack group>**↵ where **<type>** **ds1** or **ds3**. **<circuit pack group>** **g1** or **g2**.
12	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac OC-3/OC-12 **STS1 Rx loss of pointer**

Probable cause

The system is unable to detect the STS1 pointer to the STS1 path overhead for one of the following reasons:

- The local transport interface card (TIC), DS1/VT mapper, or DS3/STS mapper is defective.
- The local OC-3/OC-12 optical interface is defective.
- The upstream (transmitting) TIC, DS1/VT mapper, or DS3/STS mapper is defective.
- The upstream (transmitting) OC-3/OC-12 optical interface is defective.
- For integrated digital loop carrier (IDLC) or DS1 tandem configurations, the upstream TIC, DS1/VT mapper, or DS3/STS mapper is defective.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Check for local DS1, DS3, TIC, or OC-3/OC-12 alarms. From any FWPUI screen display the list of active alarms for the local network element by entering: **alarms**↵ *A list of alarms is displayed for the local network element.*

If	Then
TIC alarms are displayed	go to step 3.
DS1, DS3, or OC-3/OC-12 alarms are displayed	go to step 6.
no DS1, DS3, TIC, or OC-3/OC-12 alarms are displayed	go to step 2.

2	Log in to the upstream network element user interface and check for a TIC, DS1, DS3, or OC-3/OC-12 alarm.

—continued—

Fac OC-3/OC-12
STS1 Rx loss of pointer (continued)

Step	Action

If	Then
TIC alarms are displayed	go to step 3.
DS1, DS3, or OC-3/OC-12 alarms are displayed	go to step 6.
no DS1, DS3, TIC, or OC-3/OC-12 alarms are displayed	contact your next level of support.

3 To determine the upstream facility source, log in to the operations controller (OPC) and open the Connection Manager tool. (See the procedure for logging in to the OPC and opening an OPC tool in *Data Administration Procedures,* 323-3001-304, in *Operations, Administration, and Provisioning*, Volume 4A.)

If the Connection Services have been enabled, the tool opens and displays tributary information. If the Connection Services have not been enabled, an informational dialog appears, and the tool closes.

4 Complete the following substeps:

a. Locate the STS-1 alarm in the right column of the Connection Manager.

b. Note the tributary information from both network elements for this STS.

5 From Table 4-12, which lists STS default mapping, determine the mapping of the TIC STS-1 facilities, such as which STS-1 facilities are connected to the TIC (port 1 or 2 or both).

Table 4-12

Configuration	FCOT	RFT	STS#
UDLC	TIC STS-1 #2	TIC STS-1 #2	2
IDLC (ABM FCOT)	DS1 G1, G2	TIC STS-1 #1	1
IDLC (TBM FCOT)	DS1 G3, G4	TIC STS-1 #1	1
Combined: IDLC UDLC	 DS1 G1, G2 TIC STS-1 #2	 TIC STS-1 #1 TIC STS-1 #2	 1 2

—continued—

Fac OC-3/OC-12
STS1 Rx loss of pointer (continued)

Step	Action

6 Complete the instructions in the following table:

If the alarm results from a	Then
DS1 problem	go to step 7
DS3 problem	go to step 9
TIC problem	go to step 11
OC-3/OC-12 problem	go to step 17

For a DS1 problem

7 Log in to the local network element (the one that raised the alarm) and display the DS1 protection switching screen by entering:

pr;dtlprot ds1↵

The detailed protection screen appears.

8 Force traffic to the protection DS1 by entering:

force op <group>↵
y↵

where

<group>	circuit pack group from which traffic is being switched: see “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.

*The screen displays an asterisk * in the* `Forced` *column.*

If this alarm	Then
clears	replace the DS1/VT mapper from which traffic was switched (see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C).
persists	contact your next level of support.

For a DS3 problem

9 Log in to the local network element (the one that raised the alarm) and display the DS3 protection switching screen by entering:

pr;dtlprot ds3↵

The detailed protection screen appears.

—continued—

Fac OC-3/OC-12
STS1 Rx loss of pointer (continued)

Step	Action

10 Force traffic to the protection DS3 by entering:

force op <group>↵
y↵

where

<group>	circuit pack group from which traffic is being switched: see “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.

*The screen displays an asterisk * in the* `Forced` *column.*

If this alarm	Then
clears	replace the DS3/STS mapper from which traffic was switched (see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C).
persists	contact your next level of support.

For a TIC problem

11 Log in to the local network element (the one that raised the alarm) and display the TIC equipment screen:

eq tic <group>↵

where

<group>	group number of the TIC: **a** or **b**.

The TIC equipment screen appears.

12 Force traffic to the secondary TIC by entering:

switch↵
y↵

The system performs the switch.

If this alarm	**Then**
clears	go to step 13.
persists	contact your next level of support.

—continued—

Fac OC-3/OC-12
STS1 Rx loss of pointer (continued)

Step	Action
13	Change the state of the TIC, from which traffic was switched, to out-of-service by entering: **eq tic <group>**↵ where <group> group number of the TIC: **a** or **b**. *The TIC equipment screen appears.* Enter: **chgstate oos**↵ **y**↵ *The TIC card goes out-of-service.*
14	Run an out-of-service diagnostic test on the TIC. See "Performing a manual diagnostic test" on page 8-10 in this document.

If the test	Then
passes	go to step 15.
fails	go to step 16.

15	If the alarm clears, mark and monitor the pack for future failures. If it fails again, replace the pack. If the alarm persists, go to step 16.
16	Replace the TIC from which traffic was switched. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. If the alarm does not clear, contact your next level of Nortel Networks support.

For an OC-3/OC-12 problem

Note: An OC-3/OC-12 problem initiates a switch to the protection circuit pack. This switch causes a maximum traffic outage of 60 ms.

17	Look for an optical signal degrade or optical bit error rate (BER) alarms by entering: **alarms**↵
18	If the protection switch initiated by the system clears the alarm, replace the circuit pack from which the switch occurred. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. If the switch did not clear the alarm, go to step 19.

—continued—

Fac OC-3/OC-12
STS1 Rx loss of pointer (continued)

Step	Action
19	Switch the equipment on which the STS-1 originates at the far end of the fiber optics. If the protection switch clears the alarm, replace the card at the far end. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. If the protection switch does not clear the alarm, go to step 20.
20	Verify the synchronization of the network elements between the 2 end points of the facility. Make sure all network elements are synchronized to a proper source and settings.
21	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac OC-3/OC-12 **STS1 Rx unequipped**

Probable cause

A VT-managed STS-1 connection exists that has no VT1.5 traffic within it. This situation can occur for the following reasons:

- a VT-managed STS-1 connection has not been provisioned from the OPC Connection Manager
- when the last VT1.5 connection is deleted within a VT-managed STS-1 connection

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Use the Connection Manager tool on the OPC to perform one of the following actions:

- to provision one or more VT1.5 connections within the affected VT-managed STS-1 connection
- to delete the affected VT-managed STS-1 connection

—end—

Fac STS1
Line Rx BCV threshold 1, 2
Line Rx BES threshold 1, 2
Line Rx BSES threshold 1, 2
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2
Line Rx UAS threshold 1, 2

Probable cause

STS-1 performance threshold has been crossed on one of the metallic facilities. The following performance-monitoring parameters are provided:

- BCV: bipolar coding violation
- BES: bipolar errored seconds
- BSES: bipolar severely errored seconds
- CV: code violation
- ES: errored second
- SES: severely errored second
- UAS: line unavailable seconds

One of the following conditions exists:

- a faulty STS-1 input cable or connector
- a failed STS-1 interface circuit pack
- a problem with the source of the STS-1 signal

—continued—

Fac STS1
Line Rx BCV threshold 1, 2
Line Rx BES threshold 1, 2
Line Rx BSES threshold 1, 2
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2
Line Rx UAS threshold 1, 2 (continued)

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Note 1: It is assumed that these alarms have been provisioned as alarms and are turned on (activated). If not, these alarms show up as performance alerts.

Note 2: These alarms indicate that errors in excess of a provisioned level have been observed. Threshold crossing alarms will automatically clear at the end of the provisioned interval.

Action

Note 1: This procedure is service affecting.

Note 2: See *Performance Monitoring Description*, 323-3001-105, in *Description,* Volume 2A, for more information on performance-monitoring thresholds.

Step	Action
1	Locate the STS-1 port connectors on the BNC I/O circuit pack allocated to the port reporting the errors. Examine the STS-1 cable connected to the In connector of the concerned STS-1 port. Make sure that the correct connector is used and is well secured at the source and at the BNC I/O circuit pack. Do the following: **If** — **Then** the cable is split or damaged — replace it. the problem persists — go to step 2.

—continued—

Fac STS1
Line Rx BCV threshold 1, 2
Line Rx BES threshold 1, 2
Line Rx BSES threshold 1, 2
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2
Line Rx UAS threshold 1, 2 (continued)

Step	Action

2

CAUTION
Risk of service loss
Make sure that the correct STS-1 cable is unplugged. Removing the wrong one will cause another STS-1 signal to be lost.

Unplug the input STS-1 cable from the BNC I/O circuit pack and connect it to a STS-1 receiver test set. Verify that a STS-1 signal is present on the cable and that the test set does not detect any errors.

Do the following:

If	Then
no errors are detected	reconnect the STS-1 cable and go to step 4.
errors are detected	go to step 3.

3 If errors were detected at the BNC I/O circuit pack (in step 2) verify the signal at the source with the STS-1 test set.

Do the following:

If	Then
errors are detected	repair the source generating the STS-1 signal
errors are not detected	repair the STS-1 cable. Go to step 6.

—continued—

Fac STS1
Line Rx BCV threshold 1, 2
Line Rx BES threshold 1, 2
Line Rx BSES threshold 1, 2
Line Rx CV threshold 1, 2
Line Rx ES threshold 1, 2
Line Rx SES threshold 1, 2
Line Rx UAS threshold 1, 2 (continued)

Step	Action

4

CAUTION
Risk of service loss
Make sure that the proper BNC I/O circuit pack is removed. Removing the wrong circuit pack will cause another STS-1 signal to be lost. Replacing the BNC I/O circuit pack will also cause the loss of the STS-1 signal being sent on the Out side of the concerned port.

At this point the STS-1 cable and the STS-1 signal source have been verified. If errors are still occurring, then replace the BNC I/O circuit pack associated with this port. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C, for replacement instructions.

5 If the problem persists, replace the STS-1 circuit pack carrying this facility. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance,* Volume 5C, for replacement instructions.

6 If the problem continues to persist, contact your next level of support.

—end—

Fac STS1
Loopback

Probable cause

An STS-1 loopback has been operated and is currently active.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action
1	This is a normal indication when the loopback is ON for testing purposes. No action is required if this is the case.
2	To clear the alarm, release the loopback by entering: **facility sts1 <unit> <port #>** ↵ **loopback re** ↵ where **<unit>** is the circuit pack group): **g1** to **g4**. **<port #>** is **1** to **3**, or **all**.
3	If you want to put the STS-1 facility back in service, type: **chgstate is** ↵ See *Provisioning and Operations Procedures*, 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B, for more details. **—end—**

Fac STS1
Rx bipolar violation >10E-3

Probable cause

Bipolar violations have been detected on the incoming STS-1 line. One of the following conditions exists:

- a faulty coaxial connector
- a defective cable
- defective STS-1 source equipment
- a defective STS-1 interface circuit pack
- a defective signal

Note: This alarm is masked by the "Rx loss of signal" alarm.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Note: This procedure is service affecting.

Step	Action
1	Locate the STS-1 port connectors on the BNC I/O circuit pack allocated to the port reporting the errors. Examine the STS-1 cable connected to the In connector of the concerned STS-1 port. Make sure that the correct connector is used and is well secured at the source and at the BNC I/O circuit pack. Do the following:

If	Then
the cable is split or damaged	replace it.
the problem persists	go to step 2.

—continued—

Fac STS1
Rx bipolar violation >10E-3 (continued)

Step	Action

2

CAUTION
Risk of service loss
Make sure that the correct STS-1 cable is unplugged. Removing the wrong one will cause another STS-1 signal to be lost.

Unplug the input STS-1 cable from the BNC I/O circuit pack and connect it to a STS-1 receiver test set. Verify that a STS-1 signal is present on the cable and that the test set does not detect any errors.

Do the following:

If	Then
errors are detected	reconnect the STS-1 cable and go to step 4.
errors are not detected	go to step 3.

3 If errors were detected at the BNC I/O circuit pack (in step 2) verify the signal at the source with the STS-1 test set.

Do the following:

If	Then
errors are detected	repair the source generating the STS-1 signal.
errors are not detected	repair the STS-1 cable. Go to step 6.

4

CAUTION
Risk of service loss
Make sure that the proper BNC I/O circuit pack is removed. Removing the wrong circuit pack will cause another STS-1 signal to be lost. Replacing the BNC I/O circuit pack will also cause the loss of the STS-1 signal being sent on the Out side of the concerned port.

At this point the STS-1 cable and the STS-1 signal source have been verified. If errors are still occurring, then replace the BNC I/O circuit pack associated with this port. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

—continued—

Fac STS1
Rx bipolar violation >10E-3 (continued)

Step	Action
5	If the problem persists, replace the STS-1 circuit pack carrying this facility. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.
6	If the problem continues to persist, contact your next level of support.

—end—

Fac STS1
Rx loss of frame

Probable cause

The STS-1 frame cannot be detected on the incoming STS-1. One of the following conditions exists:

- defective STS-1 source equipment
- a defective cable or connection
- a defective STS-1 electrical interface circuit pack
- a defective BNC I/O circuit pack
- a faulty signal

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Locate the STS-1 port connectors on the BNC I/O circuit pack allocated to the port reporting the loss of frame. Examine the STS-1 cable connected to the In connector of the concerned STS-1 port. Make sure that the correct connector is used and is well secured at the source and at the BNC I/O circuit pack. Do the following:

If	Then
the cable is split or damaged	replace it.
the problem persists	go to step 2.

—continued—

Fac STS1
Rx loss of frame (continued)

Step	Action

2

CAUTION
Risk of service loss
Make sure that the correct STS-1 cable is unplugged. Removing the wrong one will cause another STS-1 signal to be lost.

Unplug the input STS-1 cable from the BNC I/O circuit pack and connect it to a STS-1 receiver test set. Verify that a STS-1 signal is present on the cable and that the test set does not detect a loss of frame.

Do the following:

If	Then
no loss of frame is detected	reconnect the STS-1 cable and go to step 4.
a loss of frame is detected	go to step 3.

3 Do the following:

If	Then
a loss of frame was detected at the BNC I/O circuit pack (in step 2)	verify the signal at the source with the STS-1 test set.
a loss of frame is detected	repair the source generating the STS-1 signal.
no loss of frame is detected	repair the STS-1 cable. Go to step 6.

—continued—

Fac STS1
Rx loss of frame (continued)

Step	Action

4

CAUTION
Risk of service loss
Make sure that the proper BNC I/O circuit pack is removed. Removing the wrong circuit pack will cause another STS-1 signal to be lost. Replacing the BNC I/O circuit pack will also cause the loss of the STS-1 signal being sent on the Out side of the concerned port.

At this point the STS-1 cable and the STS-1 signal source have been verified. If loss of frame is still occurring, then replace the BNC I/O circuit pack associated with this port. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

5 If the problem persists, replace the STS-1 circuit pack carrying this facility. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

6 If the problem continues to persist, contact your next level of support.

—end—

Fac STS1
Rx loss of pointer

Probable cause

The STS-1 pointer is corrupted (equivalent to losing frame) due to:

- defective far-end tributary circuit pack
- defective local STS-1 electrical interface circuit pack
- defective far-end OC-3/OC-12 optical interface circuit pack
- defective local OC-3/OC-12 optical interface circuit pack

Impact

This is a major, service-affecting (M, SA) alarm.
Switch to protection is initiated, resulting in a traffic outage of 60 ms maximum.

Action

Step	Action
1	Look for an optical signal degrade or BER alarms by entering: **alarms** ↵
2	Check if a protection switch of the equipment on which the alarm was detected clears up the problem, then replace the card. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for the appropriate procedure. Otherwise, go to step 3.
3	Check if a protection switch of the equipment on which the STS-1 originates at the far end of the coaxial cable clears the problem, then replace the card. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

—end—

Fac STS1
Rx loss of signal

Probable cause

The STS-1 frame cannot be detected on the incoming STS-1. One of the following conditions exists:

- defective STS-1 source equipment
- a defective cable or connection
- a defective STS-1 electrical interface circuit pack
- a defective BNC I/O circuit pack
- a faulty signal

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Locate the STS-1 port connectors on the BNC I/O circuit pack allocated to the port reporting the loss of signal. Examine the STS-1 cable connected to the In connector of the concerned STS-1 port. Make sure that the correct connector is used and is well secured at the source and at the BNC I/O circuit pack. Do the following:

If	Then
the cable is split or damaged	replace it
the problem persists	go to step 2

—continued—

Fac STS1
Rx loss of signal (continued)

Step	Action

CAUTION
Risk of service loss
Make sure that the correct STS-1 cable is unplugged. Removing the wrong one will cause another STS-1 signal to be lost.

2 Unplug the input STS-1 cable from the BNC I/O circuit pack and connect it to a STS-1 receiver test set. Verify that a STS-1 signal is present on the cable and that the test set does not detect a loss of signal.

Do the following:

If	Then
no loss of signal is detected	reconnect the STS-1 cable and go to step 4
a loss of signal is detected	go to step 3

3 Do the following:

If	Then
a loss of signal was detected at the BNC I/O circuit pack (in step 2)	verify the signal at the source with the STS-1 test set
a loss of signal was detected	repair the source generating the STS-1 signal
no loss of signal was detected	repair the STS-1 cable needs to be repaired. Go to step 6.

—continued—

Fac STS1
Rx loss of signal (continued)

Step	Action

CAUTION
Risk of service loss
Make sure that the proper BNC I/O circuit pack is removed. Removing the wrong circuit pack will cause another STS-1 signal to be lost. Replacing the BNC I/O circuit pack will also cause the loss of the STS-1 signal being sent on the Out side of the concerned port.

4 At this point the STS-1 cable and the STS-1 signal source have been verified. If loss of signal is still occurring, then replace the BNC I/O circuit pack associated with this port. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

5 If the problem persists, replace the STS-1 circuit pack carrying this facility. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

6 If the problem continues to persist, contact your next level of support.

—end—

Fac STS1
Rx Line AIS

Probable cause

The external equipment is experiencing signal problems and is sending a STS-1 alarm indication signal (AIS) to the STS 1 equipment.

Impact

This is a warning, service-affecting (w, SA) alarm.

Action

Step	Action
1	Verify the external equipment connected to the shelf, by connecting an STS-1 test set to the output of the source.

—end—

Fac STS1
Rx RFI

Probable cause

A Remote Failure Indication (RFI) alarm is raised when a remote defect indication condition is received from the far-end node originating the STS-1 line signal. The remote defect indication condition is sent because an STS1 LOS, STS1 LOF, or STS1 Line AIS is received on the STS-1 line signal at the far end.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	Check for STS1 LOS, STS1 LOF, or STS1 Line AIS on the far-end node where the STS1 line signal originates. Clear the alarms according to the appropriate alarm clearing procedures in this document.
2	If the alarm persists, contact your next level of support.

—end—

Fac STS1
STS1 Rx AIS

Probable cause

The local equipment is receiving an STS-1 alarm indication signal (AIS) from the coaxial cable (STS-1 signal source). One of the following conditions exists:

- a defective local STS-1 circuit pack
- a defective local STS-1 BNC I/O circuit pack
- a loose or defective coaxial cable or connector
- a signal failure at the far end of the coaxial cable

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	Verify that the facility is in service by checking the screen by entering: **facility <sts1> <circuit pack group> <port no.>** ↵ where **<circuit pack>** is the circuit pack group: **g1** to **g4**. **<port no.>** is the port number of the alarmed facility: **1** to **3**.
2	From the network element user interface, perform a manual switch on the STS-1 electrical interface circuit pack. **protectn** ↵ **dtlprot sts1** ↵ **manual op <circuit pack group>** ↵ **yes** ↵ where **<circuit pack>** is the STS-1 interface serving the facility in the alarm: **g1** to **g4**. See *Protection Switching Procedures*, 323-3001-311, in *Operations, Administration, and Provisioning*, Volume 4B, for more details.

—continued—

Fac STS1
STS1 Rx AIS (continued)

Step	Action
3	If the alarm clears, replace the defective STS-1 electrical interface circuit pack. Refer to *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions. If the problem persists, go to step 4.
4	Release the manual switch. **protectn** ↵ **dtlprot sts1** ↵ **manual re <circuit pack group>** ↵ **yes** where **<circuit pack>** **g1** to **g4** as determined in step 2.
5	Locate the STS-1 port connectors BNC I/O circuit pack allocated to the port reporting the STS1 Rx AIS. Examine the STS-1 cable connected to the “IN” connector of the concerned STS-1 port. Make sure that the correct connector is used and is well secured at the source and at the STS-1 BNC I/O circuit pack. If the cable is split or damaged, replace it. If the problem persists, go to step 6.
6	**CAUTION** **Risk of service loss** Make sure that the proper STS-1 cable is removed. Removing the wrong cable causes another STS-1 signal to be lost. Unplug the input STS-1 cable from the STS-1 BNC I/O circuit pack and connect it to a STS-1 receiver test set. Verify that a STS-1 signal is present on the cable and that the test set does not detect any errors. If there are no errors, then reconnect the STS-1 cable and go to step 8. Otherwise, go to step 7.
7	If errors were detected at the STS-1 BNC I/O circuit pack (in step 6) verify the signal at the source with the STS-1 test set. If there are errors, then the source generating the STS-1 signal should be repaired. If there are no errors, go to step 8.

—continued—

Fac STS1
STS1 Rx AIS (continued)

Step	Action

8

CAUTION
Risk of service loss
Make sure that the proper STS-1 BNC I/O circuit pack is removed. Removing the wrong circuit pack causes another STS-1 signal to be lost. Replacing the STS-1 BNC I/O circuit pack also causes the loss of the STS-1 signal being sent on the Out side of the concerned port.

At this point, the STS-1 electrical interface circuit pack, the STS-1 cable, and the STS-1 signal source have been verified. If errors are still occurring, then replace the BNC I/O circuit pack associated with this port. Refer to *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for replacement instructions.

9 If the alarm is still active, contact your next level of support.

—end—

Fac TIC
PRI link OOS

Probable cause

Data Direct's ISDN primary link interface (PRI) is out of service (OOS).

Impact

This is a major, service affecting alarm (M, SA).

Action

Step	Action
1	Display the DS1 facility for the PRI links and make sure the status is in service.
2	If the status is OOS, or if the facility does not exist, put the facility in service. For directions, see *Provisioning and Operations Procedures*, 323-2001-310, in *Operations, Administration, and Provisioning*, Volume 4B.
3	If the problem persists, contact your next level of support.

—end—

Fac TIC
STS1 Rx RFI

Probable cause

An alarm condition exists at the receiving facility.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	This alarm indicates a failure at the far end. To determine the upstream facility source, log in to the operations controller (OPC) and open the Connection Manager tool. If you do not know how to do this, see the procedure for logging in to the OPC and opening an OPC tool in *Data Administration Procedures,* 323-3001-304, in *Operations, Administration, and Provisioning*, Volume 4A. If the Connection Services have been enabled, the tool opens and displays tributary information. Go to step 2. If the Connection Services have not been enabled, an informational dialog appears, and the tool closes. Go to step 3.
2	Locate the STS-1 alarm in the right column of the Connection Manager. Note the tributary information from both network elements for this STS. Go to step 4.
3	From Table 4-13, determine the mapping of the TIC STS-1 facilities.

Table 4-13
Default mapping

Configuration	FCOT	RFT
UDLC	TIC STS-1 #2	TIC STS-1 #2
GR-303 (ABM FCOT)	DS1 G1, G2	TIC STS-1 #1
GR-303 (TBM FCOT)	DS1 G3, G4	TIC STS-1 #1
Combined: GR-303 UDLC	 DS1 G1, G2 TIC STS-1 #2	 TIC STS-1 #1 TIC STS-1 #2

4	Clear the TIC, OC-3/OC-12, or DS1 equipment or facility alarm at the transmitting network element.
5	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac TIC
STS1 Rx unequipped

Probable cause

Alarm raised on an AccessNode access bandwidth manager shelf

The TIC is not receiving an STS-1 payload from the upstream TIC or DS1 for one of the following reasons:

- in a UDLC configuration, the upstream TIC STS-1 facilities are out of service (OOS)
- in a GR-303 or DS1 Tandem configuration, the upstream DS1 facilities are out of service, or the DS1/VT mapper is faulty
- in a combined configuration, any of the above two conditions may pertain

Alarm raised on an AccessNode Express host digital terminal

The TIC is not receiving an STS-1 payload from the upstream TIC or DS1 for the following reason:

- in a host digital terminal (HDT) with an operations controller (OPC), mapper slots 5 and 6 do not contain DS1/VT mapper circuit cards and are out of service (OOS), as the OPC is placed in mapper slots 5 through 8

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Determine if the alarm is raised on an AccessNode access bandwidth manager (ABM) shelf or an AccessNode Express HDT.

If the alarm is raised on	Then
an ABM shelf	go to step 2.
an HDT	go to step 21.

2	To determine the upstream facility alarm source, log in to the OPC and open the Connection Manager tool. ***Note:*** If you do not know how to do this, see the procedure for logging in to the OPC and opening an OPC tool in *OPC User Interface Description,* 323-3001-301, in *Operations, Administration, and Provisioning*, Volume 4A.
3	If the Connection Services have been enabled, the tool will open and display tributary information. Go to step 4. If the Connection Services have not been enabled, an informational dialog will inform you of this, and the tool will close. Go to step 5.

—continued—

Fac TIC
STS1 Rx unequipped (continued)

Step	Action

4 Locate the STS-1 alarm in the right-hand column of the Connection Manager. Note the tributary information from both network elements for this STS. Go to step 6.

5 From the following table (default mapping), determine the mapping of the TIC STS-1 facilities, such as which STS-1 facilities are connected to the TIC (port 1 and/or 2.

Default mapping

Configuration	FCOT	RFT
UDLC	TIC STS-1 #2	TIC STS-1 #2
GR-303 (ABM FCOT)	DS1 G1, G2	TIC STS-1 #1
GR-303 (TBM FCOT)	DS1 G3, G4	TIC STS-1 #1
Combined: GR-303 UDLC	 DS1 G1, G2 TIC STS-1 #2	 TIC STS-1 #1 TIC STS-1 #2

6 Check the configuration.

If configuration is	Then
UDLC	go to step 7.
GR-303	go to step 14.
Combined UDLC traffic	go to step 7.
Combined GR-303 traffic	go to step 14.

UDLC or combined UDLC traffic configuration

7 Log in to the upstream network element user interface and display the UDLC, TIC STS-1 facility screen:

fa tic 2↵

The TIC facility screen appears, showing the STS-1 # state.

If the STS-1 # state is	Then
OOS	there is a possible software error. Go to step 22.
IS	go to step 8.

—continued—

Fac TIC
STS1 Rx unequipped (continued)

Step	Actions

8 Perform a protection switch on the upstream TIC:

a. From the Network Element Status screen, display the required TIC equipment screen:

eq tic <plane>↵

where

<plane> is the plane of the TIC: **a** or **b**.

The TIC equipment screen appears.

b. Switch to the backup circuit pack:

switch↵

y↵

The system performs the switch.

c. Did the alarm clear?

If	Then
yes	go to step 9
no	go to step 14

9 Change the state of the TIC, from which traffic was switched, to out-of-service:

eq tic <plane>↵

where

<plane> is the plane of the TIC: **a** or **b**.

The TIC equipment screen appears.

chgstate oos↵
y↵

The TIC card goes out of service.

10 Run an out-of-service diagnostic test on the TIC. See “Performing a manual diagnostic test” on page 8-10 in this document.

If the alarm	Then
clears	mark the TIC and monitor it for further failure. If the TIC fails again, replace the TIC as described in step 11. End the procedure.
persists	go to step 11.

—continued—

Fac TIC
STS1 Rx unequipped (continued)

Step	Action
11	Replace the TIC from which service was switched, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance*, Volume 5C.
12	Log in to the network element user interface (NEUI).
13	Did the alarm clear?

If	Then
yes	end the procedure.
no	go to step 22.

GR-303 or combined GR-303 traffic configuration

14 At the upstream site, display the DS1 facility screen for the DS1 group associated with GR-303 or DS1 tandem traffic:

fa ds1 <group>↵

where

<group>	group number of the GR-303 or DS1 tandem, DS1: see “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.

The DS1 facility screen appears.

15 Query the state of all DS1 facilities (ports) associated with the circuit pack:

query↵

The state and port number appears for each DS1 facility associated with the selected DS1/VT mapper circuit pack.

If all DS1s are	Then
OOS	go to step 16.
IS	go to step 17.

—continued—

Fac TIC
STS1 Rx unequipped (continued)

Step	Action

16 Change the state of the out-of-service DS1 facilities associated with the GR-303 traffic or DS1 tandem, to in-service:

select <group> <port>

where

<group>	is the group number of the GR-303 or DS1 tandem, DS1: see “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.
<port>	is the DS1 facility associated with the circuit pack.

chgstate is↵

y↵

Repeat this step for each DS1 facility to be returned to in-service.

The state of the DS1 facility changes to in-service (IS).

If the alarm	Then
clears	end the procedure
persists	go to step 17

17 Perform a protection switch on the upstream GR-303 DS1/VT mapper:

a. From the Network Element Status screen, display the DS1 protection switching screen:

pr;dtlprot ds1↵

The DS1 detailed protection switching screen appears.

b. Operate the manual switch:

manual op <group>↵
y↵

where

<group>	is the number of the DS1 group: see “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.

When a manual switch is operated, the screen displays an asterisk (*****) in the `Manual` *column.*

If the alarm	Then
clears	go to step 18
persists	go to step 19

—continued—

Fac TIC
STS1 Rx unequipped (continued)

Step	Action

18 Replace the DS1/VT mapper from which service was switched, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. End the procedure.

19 At the upstream site, perform a protection switch on the working OC-12:

a. Display the OC-3/OC-12 protection switching screen:

pr;dtlprot <type>↵

where

<type> is the type of optics: **oc3** or **oc12**.

The detailed protection screen appears.

b. Operate the manual switch:

manual op <group>↵
y↵

where

<group> OC-3/OC-12 circuit pack group from which traffic is being switched: **g1** or **g2**.

*The screen displays an asterisk ***** in the* `Manual` *column.*

If this alarm	Then
clears	go to step 20.
persists	go to step 22.

20 Replace the OC-3/OC-12 upstream optical interface, from which service was switched in step 19, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance*, Volume 5C. Go to step 22.

21 Disable the TIC/STS-1 alarms associated with mapper slots 5 and 6 on the HDT. For instructions on how to disable TIC/STS-1 alarms, see the *AccessNode Express Commissioning Quick Reference Guide*.

22 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac TIC
TR-08 System [1 … 21] far end major

Probable cause

A DS1 facility between the FCOT and the local digital switch has failed. There is still communication between the local digital switch and the TIC, but DS1 traffic is lost. The failed DS1 facility is associated with a TR-08 system from 1 to 21.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Check the local digital switch for TR-08 alarms and check the DS1 facility between the FCOT and the local digital switch for faulty connections or damaged cable. Also, ensure that the local digital switch has the correct hardware and provisioning to support TR-08.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac TIC
TR-08 System [1 … 21] loss of Rx DDL

Probable cause

This alarm is caused by any of the following fault conditions:

- The version of the TIC or DS1/VT mapper circuit pack that is installed in the shelf does not support TR-08. If this is true, there will be a corresponding “Epq TIC, TR-08 Circuit pack mismatch alarm.”
- A DS1 facility associated with a TR-08 system from 1 to 21 does not have the framing format set to DLC.
- The DS1 signal coming from the local digital switch has a loss of frame (LOF) condition.

Impact

This is a major, service-affecting (M, SA) alarm.

—continued—

Fac TIC
TR-08 System [1 … 21] loss of Rx DDL (continued)

Action

Step	Action
1	Check for TR-08 circuit pack mismatch alarms at the RFT. Display the list of active alarms for the RFT by entering the following command from the FWPUI screen: **alarms**↵

If there is	Then
a TR-08 circuit pack mismatch alarm	ensure that the TIC at the RFT is an NT4K56AC card or later and the DS1/VT mapper at the FCOT is an NT7E04CA or later card. If necessary, replace the TIC and the DS1/VT mapper with the correct cards as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. (See step 10 in this procedure, for details on finding the slot location of the DS1/VT mapper card.)
no TR-08 circuit pack mismatch alarm	go to step 2.

Step	Action
2	From the RFT network element status screen, check for other TIC alarms by entering: **alarms**↵

If there are	Then
TIC alarms	clear the alarm using the appropriate alarm clearing procedures in this book. Go to step 3.
no TIC alarms	go to step 4.

—continued—

Fac TIC
TR-08 System [1 … 21] loss of Rx DDL (continued)

Step	Action

3 From the FCOT, check for DS1/VT mapper alarms.

If there are	Then
DS1/VT mapper alarms	refer to the appropriate alarm procedures in this document to clear the alarms. Go to step 4.
no DS1/VT mapper alarms	go to step 4.

4 From the RFT network element status screen, display the equipment screen for the TIC:

eq tic <plane>↵

where

<plane> plane of the primary TIC: **a** or **b**.

The TIC equipment screen appears.

If diagnosing a	Then
primary in-service TIC	go to step 5.
secondary in-service TIC	go to step 6.

5 Switch service from the primary TIC to the secondary TIC.

switch↵

The system prompts for confirmation of the state change.

y↵

6 Change the state of the TIC to out-of-service (OOS) to perform a complete diagnostic:

chgstate oos↵

The system prompts for confirmation of the state change.

y↵

—continued—

Fac TIC
TR-08 System [1 … 21] loss of Rx DDL (continued)

Step	Action
7	Perform a manual diagnostic on the TIC. For details, see the chapter "Performing diagnostic tests" in this document.

If the test result is	Then
Diag Pass	go to step 8.
Diag Fail	replace the TIC as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. Go to step 8.

8	Put the TIC in-service (IS) by entering: **chgstate is**↵ *The system prompts for confirmation of the state change.* **y**↵
9	Determine if the TR-08 System <n> loss of Rx DDL alarm clears.

If this alarm	Then
clears	you have finished the procedure.
persists	ensure the DS1/VT mapper in the FCOT is properly seated in its slot by performing the following steps. Go to step 10.

10	Determine the slot location of the DS1/VT mapper circuit pack associated with this alarm using the OPC Facility Assignment Manager (FAM) tool. Using FAM, find the A-link for TR-08 system <n>, where n is the system number referred to in this alarm. For details see *Provisioning and Operations Procedures,* 323-3001-310, in *Operations, Administration, and Provisioning*, Volume 4B*.*
11	From the Network Element Status screen, display the DS1 protection screen: **pr;dtlprot ds1**↵

—continued—

Fac TIC
TR-08 System [1 … 21] loss of Rx DDL (continued)

Step	Action
12	Switch service to the protection DS1/VT mapper circuit pack: **manual op <group>**↵ **y**↵ where <group> group number of the DS1/VT mapper being replaced. “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15 for values
13	Unseat then reseat the DS1/VT mapper card as follows: **a.** Remove the shelf cover. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for details. **b.** Pull the circuit pack ejector latches to disengage the circuit pack from the backplane connector and slide the circuit pack about 1 inch (25.4 mm) out of its slot. **c.** Wait at least 5 seconds before reseating the DS1/VT mapper. Gently push the DS1/VT mapper in until the ejector latches come in contact with the shelf. Then push the latches in toward the circuit pack to engage the circuit pack with the backplane connector.
14	If the automatic-in-service feature is set to on, and the circuit pack state automatically changes to in-service (IS), skip to step 16.
15	From the DS1 equipment screen, change the state of the reseated DS1/VT mapper to in-service (IS): **chgstate is**↵

—continued—

Fac TIC
TR-08 System [1 … 21] loss of Rx DDL (continued)

Step	Action
16	From the detailed protection screen, release the protection switch: **manual re <group>**↵ **y**↵ where <group> is the group number of the reseated DS1/VT mapper. See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15 for values. *When a protection switch is released, the screen displays a period (.) in the manual column.*
17	Replace the shelf cover. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C, for details.
18	Determine if the TR-08 System <n> loss of Rx DDL alarm clears

If this alarm	Then
clears	you have finished the procedure
persists	Check the frame format by performing the following steps. Go to step 19.

19	From the Network Element Status screen, display the DS1 facility provisioning screen: **fa ds1 <group><port>**↵ where group is the DS1 group number. See “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15 for values. port is the number of the DS1 port: **1** to **14**, or **all**. *The DS1 facility provisioning screen appears.*

—continued—

Fac TIC
TR-08 System [1 … 21] loss of Rx DDL (continued)

Step	Action
20	On the DS1 facility provisioning screen displayed in step 19, determine the `Framing Format` for the DS1 facility.

If the framing format is	Then
DLC	Use a DS1 test set to check the stability of the DS1 signal from the local digital switch. If the problem can not be identified, contact Nortel Networks Customer Service for assistance
not DLC	go to step 21

21	Take the DS1 facility out of service: **chgstate oos**↵ **y**↵ *The state of the DS1 facility changes to out-of-service (00S).*
22	Provision the framing format appropriate to TR-08: **edit;framefmt dlc**↵ *The provisioned value appears in reverse video*
23	Return the facility to service: **quit;chgstate is**↵ *The state changes to in-service (IS).*
24	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac TIC
TR-08 System [1 … 21] Rx fail

Probable cause

There is a loss of signal on the DS1, which connects the FCOT to the local digital switch.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Log in to the FCOT and check for equipment or facility alarms raised against the DS1 equipment that corresponds to systems 1 to 21. Look up the alarm in this document and proceed accordingly.

If the problem cannot be corrected at the FCOT, check all cables, connections, and service states at the local digital switch.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac TIC
VT Path signal label mismatch

Probable cause

The VT signal label is not set the same for each end of the facility.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action

1 Check for synchronization between the near end and far end. The following combinations of received (far end) and provisioned (near end) signals will result in an alarm:

Received	Provisioned	Mismatch (Y/N)
byte synchronous	asynchronous	Y
asynchronous	byte synchronous	Y

Note 1: No signal label mismatch is generated if the Received label is unequipped.

Note 2: No VT path signal label mismatch alarm is generated if the VTs on the TIC are unequipped; that situation would generate a VT Rx unequipped alarm.

2 Change the synchronization of either end to the appropriate setting, so that it is the same as the other end.

Note: A VT signal label mismatch alarm provides downstream conditioning and generates a VT Rx RFI on the downstream equipment. Once the VT path service level alarm is removed, the VT Rx RFI on the downstream equipment will also be removed.

3 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac TIC
VT Rx AIS

Probable cause

The cause of this alarm depends on the type of configuration or mode of the system. Causes include the following:

- The facility that reports the AIS alarm is receiving an Alarm Indication Signal.
- **In a UDLC configuration,** an alarm condition exists at either the upstream (transmitting) transport interface card (TIC) or access interface card (AIC).
- **In a GR-303 or DS1 Tandem configuration,** an alarm condition exists at the upstream (transmitting) DS1/VT mapper.
- **In a combined configuration,** an alarm condition exists either at the upstream transport interface card (TIC), at the access interface card (AIC), or at the upstream DS1/VT mapper.
- **In asynchronous mode,** the alarm is caused by one of the following conditions (go to step for action):
  - — Framing format is not set the same for each end of the facility.
  - — Framing format is corrupted.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

—continued—

Fac TIC
VT Rx AIS (continued)

Action

Step	Action

All conditions except asynchronous mode

1 Identify which VT in which STS is alarmed.

Note: When an STS-1 is posted at the map, the VTs are numbered 1 to 28. Alarms for VTs, however, are numbered sequentially from 1 to 336; the following table and rule-of-thumb can help determine which STS houses a particular VT.

VT in alarm	STS number	VT in alarm	STS number
1 to 28	1	168 to 196	7
29 to 56	2	197 to 224	8
57 to 84	3	225 to 252	9
85 to 112	4	253 to 280	10
113 to 140	5	281 to 308	11
141 to 168	6	309 to 336	12

—continued—

Fac TIC
VT Rx AIS (continued)

Step	Action
2	To determine which STS/VT is in alarm: **a.** Divide 28 into the number of the VT that is reported. ***Example***: If VT 98 is in alarm: *28 divides into 98 three times (98 ÷ 28 = 3 remainder 14)* This whole number (if it has a remainder) plus one equals the STS in which the VT resides. *Add one to this answer: 3 + 1 = 4. So,'VT 98' is on STS #4.* **b.** The 'remainder' indicates the VT that is in alarm in that STS. The remainder (98 – 84 = 14) is the VT, which is 14. (If there is no remainder [e.g. 84 ÷ 28 = 3] the VT is the last one in that STS [84 is the last VT in STS #3, i.e. VT #28.]) *Thus, VT 98 is on STS #4, VT 14 at the facility TIC level.*
3	To determine the upstream facility source, log in to the OPC and open the Connection Manager tool. ***Note:*** If you do not know how to do this, see the procedure for logging in to the OPC and opening an OPC tool in *Data Administration Procedures,* 323-3001-304, in *Operations, Administration, and Provisioning*, Volume 4A.
4	If the Connection Services have been enabled, the tool will open and display tributary information. Go to step.5 If the Connection Services have not been enabled, an informational dialog will inform you of this, and the tool will close. Go to step 6.
5	Locate the STS-1 alarm in the right-hand column of the Connection Manager. Note the tributary information from both network elements for this STS. Go to step 7.
6	From the following table (default mapping), determine the mapping of the TIC STS-1 facilities, such as which STS-1 facilities are connected to the TIC (port 1 and/or 2).

—continued—

Fac TIC
VT Rx AIS (continued)

Step Action

Default mapping

Configuration	FCOT	RFT	STS#
UDLC	TIC STS-1 #2	TIC STS-1 #2	2
GR-303 (ABM FCOT)	DS1 G1, G2	TIC STS-1 #1	1
GR-303 (TBM FCOT)	DS1 G3, G4	TIC STS-1 #1	1
Combined: GR-303 UDLC	 DS1 G1, G2 TIC STS-1 #2	 TIC STS-1 #1 TIC STS-1 #2	 1 2

7 Log in to the network element user interface at the upstream network element and check for the following:

a. In a UDLC configuration, check the upstream (transmitting) network element for TIC or AIC equipment, or TIC or AIC facility alarms. Look up the alarm in this document, and proceed accordingly.

b. In a GR-303 or DS1 Tandem configuration, check the upstream (transmitting) network element for DS1 equipment or DS1 facility alarms. Look up the alarm in this document, and proceed accordingly.

c. In a combined configuration, check the upstream network element for TIC or AIC equipment, or TIC or AIC facility alarms, or for DS1 equipment or DS1 facility alarms. Look up the alarm in this document, and proceed accordingly.

For details on how to log in to the network element user interface and view alarms, see “Displaying alarms” on page 1-2.

8 If you cannot successfully complete this procedure, contact your next level of support.

Asynchronous mode

9 Check the far-end network element or external equipment for an equipment or facility TIC alarm.

If	Then
there is an equipment or facility alarm	look up the alarm in this document, and proceed accordingly.
there are no equipment or facility alarms	go to step 10.

—continued—

Fac TIC
Rx loss of frame (continued)

Step	Action

10 At each end of the facility, ensure that the frame format is set the same. To check the frame format, enter:

fa tic <sts #>↵

where

<sts #>	is the number of the TIC STS-1 facility: **1** to **6** (VTs 1 to 28 are on TIC STS-1 #1; VTs 29 to 56 are on #2; VTs 57 to 84 are on #3, etc.).

The TIC facility screen appears.

11 Select option 7 for subport selection (SubprtSel) and enter:

subptsel <first VT1.5 #> <last VT1.5 #>

where

<first VT1.5 #>	is the number of the first TIC VT1.5: **1** to **28**.
<last VT1.5 #>	is the number of the last TIC VT1.5: **1** to **28**.

Note: To select a single subport, enter the same number for <first VT1.5 #> and < last VT1.5 # >.

If the frame formats are	Then
set the same	go to step 13.
not the same	go to step 12.

12 Change the frame format by entering:

edit framing format <format type>

where

<format type>	is null, superframe, extended, or dlc

—continued—

Fac TIC
Rx loss of frame (continued)

Step	Action

13 From the Subport Selection screen, check the synchronization for near-end and far-end mismatched frames.

If the frames are mismatched, replace the affected DS1/VT mapper circuit pack as outlined in Module Replacement Procedures, 323-3001-547, in Maintenance, Volume 5C.

If the alarm	Then
persists	go to step 14.
clears	end the procedure.

14 At the near-end site (receiving end), check the cable between the TIC and the cross-connect for physical damage.

If the cable is	Then
good	go to step 15.
damaged	replace the cable.

15

CAUTION
Loss of service
This step takes the TIC out of service.

—continued—

Fac TIC
Rx loss of frame (continued)

Step	Action
	From the Network Element Status screen, to take the affected TIC out of service you must first take all three STS-1 facilities out of service. Enter the following: **fa tic 1**↵ **chgstate oos**↵ **y** **fa tic 2**↵ **chgstate oos**↵ **y** **fa tic 3**↵ **chgstate oos**↵ **y** **eq tic <plane>**↵ **chgstate oos**↵ **yes**↵ where <plane> is the TIC you want to take out of service: **a** or **b**.
16	Replace the TIC as outlined in *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.
17	If the alarm persists, replace the OC-12 circuit pack where the failure is reported. See *Module Replacement Procedures*, 323-3001-547 in *Maintenance*, Volume 5C.
18	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac TIC
VT Rx loss of pointer

Probable cause

The VT1.5 pointer is corrupted for one of the following reasons:

- the upstream TIC is defective (in a UDLC configuration)
- the upstream OC-3/OC-12 optical interface is defective
- the local /OC-3OC-12 optical interface is defective
- the upstream (transmitting) DS1/VT mapper is defective (in a GR-303 or DS1 Tandem configuration)

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action

1 Identify which VT in which STS is alarmed.

When an STS-1 is posted at the map, the VTs are numbered 1 to 28. Alarms for VTs, however, are numbered sequentially from 1 to 336; the following table and rule-of-thumb can help determine which STS houses a particular VT.

VT in alarm	STS number	VT in alarm	STS number
1 to 28	1	168 to 196	7
29 to 56	2	197 to 224	8
57 to 84	3	225 to 252	9
85 to 112	4	253 to 280	10
113 to 140	5	281 to 308	11
141 to 168	6	309 to 336	12

—continued—

Fac TIC
VT Rx loss of pointer (continued)

Step	Action
2	To determine which STS/VT is in alarm: **a.** Divide 28 into the number of the VT that is reported. ***Example***: If VT 98 is in alarm: *28 divides into 98 three times (98 ÷ 28 = 3 remainder 14)* This whole number (if it has a remainder) plus one equals the STS in which the VT resides. *Add one to this answer: 3 + 1 = 4. So, 'VT 98' is on STS # 4.* **b.** The 'remainder' indicates the VT that is in alarm in that STS. The remainder (98 - 84 = 14) is the VT, which is 14. (If there is no remainder [e.g. 84 ÷ 28 = 3] the VT is the last one in that STS [84 is the last VT in STS # 3, i.e. VT # 28.]) *Thus, VT 98 is on STS 4, VT 14 at the facility TIC level.*
3	To determine the upstream facility source, log in to the OPC and open the Connection Manager tool. ***Note:*** If you do not know how to do this, see the procedure for logging in to the OPC and opening an OPC tool in *Data Administration Procedures,* 323-3001-304, in *Operations, Administration, and Provisioning*, Volume 4A.
4	If the Connection Services have been enabled, the tool will open and display tributary information. Go to step 5. If the Connection Services have not been enabled, an informational dialog will inform you of this, and the tool will close. Go to step 6.
5	Locate the STS-1 alarm in the right-hand column of the Connection Manager. Note the tributary information from both network elements for this STS. Go to step 7.
6	From the following table (default mapping), determine the mapping of the TIC STS-1 facilities, such as which STS-1 facilities are connected to the TIC (port 1 and/or 2).

—continued—

Fac TIC
VT Rx loss of pointer (continued)

Step Action

Default mapping

Configuration	FCOT	RFT	STS#
UDLC	TIC STS-1 #2	TIC STS-1 #2	2
GR-303 (ABM FCOT)	DS1 G1, G2	TIC STS-1 #1	1
GR-303 (TBM FCOT)	DS1 G3, G4	TIC STS-1 #1	1
Combined: GR-303 UDLC	 DS1 G1, G2 TIC STS-1 #2	 TIC STS-1 #1 TIC STS-1 #2	 1 2

7 Log in to the upstream network element and check for OC-3/OC-12 or TIC equipment and facility alarms.

If OC-3/OC-12 or TIC alarms	Then
are present	go to step 8.
not present	go to step 9.

8 Look up the alarm in this document, and proceed to clear the alarm as instructed. End the procedure.

9 Perform a protection switch on the upstream primary TIC:

a. Display the TIC equipment screen:

eq tic <group>↵

where

<group> is the group number of primary TIC: **a** or **b**.

The TIC equipment screen appears.

b. Operate the manual switch:

switch↵
y↵

The system performs the switch.

If this alarm	**Then**
clears	go to step 12
persists	go to step 10

—continued—

Fac TIC
VT Rx loss of pointer (continued)

Step	Action
10	At the upstream site, perform a protection switch on the working OC-12: **a.** Display the OC-3/OC-12 protection switching screen: **pr;dtlprot <type>**↵ where <type> is the type of optics: **oc3** or **oc12**. *The detailed protection screen appears.* **b.** Operate the manual switch: **manual op <group>**↵ **y**↵ where <group> is the OC-3/OC-12 circuit pack group from which traffic is being switched: **g1** or **g2**. *The screen displays an asterisk ***** in the* `Manual` *column.*

If this alarm	Then
clears	go to step 12.
persists	go to step 11.

—continued—

Fac TIC
VT Rx loss of pointer (continued)

Step	Action

11 Perform a protection switch on the local primary TIC:

a. Log in to the local network element and display the TIC equipment screen:

eq tic < group >↵

where

<group> is the group number of the primary TIC: **a** or **b**.

The TIC equipment screen appears.

b. Operate the manual switch from the primary to the secondary TIC:

switch↵
y↵

The system performs the switch.

If this alarm	Then
clears	go to step 12.
persists	go to step 13.

12 Replace the circuit pack, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance*, Volume 5C.

If the alarm clears, end the procedure.

13 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac TIC
VT Rx RFI

Probable cause

The node issuing this alarm received a remote defect indication (RDI) from the far-end node that originates the virtual tributary (VT) path. The far-end node sent the RDI because it is receiving a VT alarm indication signal (AIS) or a VT loss of pointer (LOP).

In a universal digital loop carrier (UDLC) configuration, an alarm condition exists at the receiving transport interface card (TIC).

In a GR-303 or DS1 Tandem configuration, an alarm condition exists at the receiving DS1/VT mapper.

The TIC facility is indicating that there is an alarm condition at the receiving network element.

Impact

This is a warning, not service-affecting (w, nsa) alarm.

Action

Step	Action
1	Identify which VT in which STS is alarmed. When an STS-1 is posted at the maintenance and administration position (MAP), the VTs are numbered 1 to 28. Alarms for VTs, however, are numbered sequentially from 1 to 336. Table 4-14 can help determine which STS houses a particular VT.

Table 4-14

VT in alarm	STS number	VT in alarm	STS number
1 to 28	1	168 to 196	7
29 to 56	2	197 to 224	8
57 to 84	3	225 to 252	9
85 to 112	4	253 to 280	10
113 to 140	5	281 to 308	11
141 to 168	6	309 to 336	12

—continued—

Fac TIC
VT Rx RFI (continued)

Step	Action
2	To determine which STS/VT is in alarm: **a.** Divide 28 into the number of the VT that is reported. ***Example***:: If VT 98 is in alarm: *28 divides into 98 three times (98 ÷ 28 = 3 remainder 14)* This whole number (if it has a remainder) plus one equals the STS in which the VT resides. *Add one to this answer: 3 + 1 = 4. So, 'VT 98' is on STS # 4.* **b.** The 'remainder' indicates the VT that is in alarm in that STS. The remainder (98 - 84 = 14) is the VT, which is 14. (If there is no remainder [for example 84 ÷ 28 = 3] the VT is the last one in that STS [84 is the last VT in STS # 3, that is VT # 28.]) *Thus, VT 98 is on STS 4, VT 14 at the facility TIC level.*
3	To determine the upstream facility source, log in to the operations controller (OPC) and open the Connection Manager tool. If you do not know how to do this, see the procedure for logging in to the OPC and opening an OPC tool in *Data Administration Procedures,* 323-3001-304, in *Operations, Administration, and Provisioning*, Volume 4A. If the Connection Services have been enabled, the tool opens and displays tributary information. Go to step 4. If the Connection Services have not been enabled, an informational dialog appears, and the tool closes. Go to step 5.
4	Locate the STS-1 alarm in the right column of the Connection Manager. Note the tributary information from both network elements for this STS. Go to step 6.
5	From Table 4-15, determine the mapping of the TIC STS-1 facilities, such as which STS-1 facilities are connected to the TIC (port 1 or 2 or both).

—continued—

Fac TIC
VT Rx RFI (continued)

Step Action

Table 4-15
Default mapping

Configuration	FCOT	RFT	STS#
UDLC	TIC STS-1 #2	TIC STS-1 #2	2
GR-303 (ABM FCOT)	DS1 G1, G2	TIC STS-1 #1	1
GR-303 (TBM FCOT)	DS1 G3, G4	TIC STS-1 #1	1
Combined: GR-303 UDLC	 DS1 G1, G2 TIC STS-1 #2	 TIC STS-1 #1 TIC STS-1 #2	 1 2

6 Log in to the network element user interface at the receiving network element and check for the following:

a. In a UDLC configuration, check the receiving network element for TIC equipment or facility alarms. Look up the alarms in this document, and proceed accordingly.

b. In a GR-303 or DS1 Tandem configuration, check the receiving network element for DS1 equipment or facility alarms. Look up the alarms in this document, and proceed accordingly.

7 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Fac TIC
VT Rx unequipped

Probable cause

The TIC is not receiving a VT payload from the upstream TIC or DS1 for one of the following reasons:

- In a UDLC configuration this alarm can be raised for one of the following reasons:
  - — the far-end VT1.5 facility is out-of-service, and should be placed back in-service
  - — the far-end TIC is faulty
- In a GR-303 or DS1 Tandem configuration, one or more, but not all upstream DS1 facilities are out of service (OOS), or the DS1/VT mapper is faulty.
- In a combined configuration, any of the above conditions may pertain.

Impact

This is a major, service-affecting (M, SA) alarm.

Action

Step	Action
1	Identify which VT in which STS is alarmed. When an STS-1 is posted at the map, the VTs are numbered 1 to 28. Alarms for VTs, however, are numbered sequentially from 1 to 336; the following table and rule-of-thumb can help determine which STS houses a particular VT.

VT in alarm	STS number	VT in alarm	STS number
1 to 28	1	168 to 196	7
29 to 56	2	197 to 224	8
57 to 84	3	225 to 252	9
85 to 112	4	253 to 280	10
113 to 140	5	281 to 308	11
141 to 168	6	309 to 336	12

—continued—

Fac TIC
VT Rx unequipped (continued)

Step	Action
2	To determine which STS/VT is in alarm: **a.** Divide 28 into the number of the VT that is reported. ***Example***: If VT 98 is in alarm: *28 divides into 98 three times (98 ÷ 28 = 3 remainder 14)* This whole number (if it has a remainder) plus one equals the STS in which the VT resides. *Add one to this answer: 3 + 1 = 4. So,' VT 98' is on STS # 4.* **a.** The 'remainder' indicates the VT that is in alarm in that STS. The remainder (98 – 84 = 14) is the VT, which is 14. (If there is no remainder [e.g. 84 ÷ 28 = 3] the VT is the last one in that STS [84 is the last VT in STS # 3, i.e. VT # 28.]) *Thus, VT 98 is on STS 4, VT 14 at the facility TIC level.*
3	To determine the upstream facility source, log in to the OPC and open the Connection Manager tool. If you do not know how to do this, see the procedure for logging in to the OPC and opening an OPC tool in *Data Administration Procedures,* 323-3001-304, in *Operations, Administration, and Provisioning*, Volume 4A.
4	If the Connection Services have been enabled, the tool will open and display tributary information. Go to step 5. If the Connection Services have not been enabled, an informational dialog will inform you of this, and the tool will close. Go to step 6.
5	Locate the STS-1 alarm in the right-hand column of the Connection Manager. Note the tributary information from both network elements for this STS. Go to step 7.
6	From the following table (default mapping), determine the mapping of the TIC STS-1 facilities, such as which STS-1 facilities are connected to the TIC (port 1 and/or 2.

—continued—

Fac TIC
VT Rx unequipped (continued)

Step Action

Default mapping

Configuration	FCOT	RFT	STS#
UDLC	TIC STS-1 #2	TIC STS-1 #2	2
GR-303 (ABM FCOT)	DS1 G1, G2	TIC STS-1 #1	1
GR-303 (TBM FCOT)	DS1 G3, G4	TIC STS-1 #1	1
Combined: GR-303 UDLC	 DS1 G1, G2 TIC STS-1 #2	 TIC STS-1 #1 TIC STS-1 #2	 1 2

7 Check the configuration.

If configuration is	**Then**
UDLC	go to step 8.
GR-303 or DS1 tandem	go to step 15.
Combined, STS associated with UDLC traffic	go to step 8.
Combined, STS associated with GR-303 traffic or DS1 tandem	go to step 15.

8 Log in to the network element user interface of the upstream network element and display the TIC STS-1 facility screen for UDLC:

fa tic <sts#> ↵

where

<STS #> is the TIC STS-1 facility associated with the UDLC traffic

The TIC/STS-1 facility screen appears.

The status of all VT1.5s is displayed.

—continued—

Fac TIC
VT Rx unequipped (continued)

Step	Action
9	For the VT1.5 reporting this alarm, change the operating state of the VT1.5 to in-service: **vtselect < VT # >** ↵ where <VT #> is the number of the VT reporting the alarm: **1** to **28**. **chgstate is** ↵ *The TIC facility screen is updated with the new operating state in reverse video, and this alarm should clear.* **If** the alarm — **Then** clears — go to step 10. persists — go to step 11.
10	End the procedure.
11	Perform a protection switch on the upstream TIC: **a.** Display the required TIC equipment screen: **eq tic < group >**↵ where <group> is the group number of the TIC: **a** or **b**. *The TIC equipment screen appears.* **b.** Switch to the backup circuit pack: **switch**↵ **y**↵ *The system performs the switch.* **If** the alarm — **Then** clears — go to step 12. persists — go to step 21.

—continued—

Fac TIC
VT Rx unequipped (continued)

Step	Action

12 Change the state of the TIC, from which traffic was switched, to out-of-service:

eq tic < group >↵

The TIC equipment screen appears.

where

<group> is the group number of the TIC: **a** or **b**.

chgstate oos↵
y↵

The TIC card goes out of service.

13 Run an out-of-service diagnostic test on the TIC. Refer to "Performing a manual diagnostic test" on page 8-10 in this document.

If the alarm	**Then**
clears	end the procedure.
persists	go to step 14.

14 Replace the TIC from which service was switched, as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance*, Volume 5C.

End the procedure.

15 At the upstream network element, display the DS1 facility screen for the DS1 group associated with GR-303 or DS1 tandem traffic:

fa ds1 <group> all↵

where

<group> is the group number of the DS1 (GR-303 or DS1 tandem): see "Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12" on page 1-15.

The DS1 facility screen appears.

16 Query the state of all DS1 facilities (ports) associated with the circuit pack:

query↵

The state and port number appears for each DS1 facility associated with the selected DS1/VT mapper circuit pack group.

If any DS1 is	**Then**
out-of-service (OOS)	go to step 17.
in-service (IS)	go to step 19.

—continued—

Fac TIC
VT Rx unequipped (continued)

Step	Action
17	There are two courses of action: If it is okay to do so, change the state of all DS1 facilities that are in alarm and incorrectly changed to the out-of-service state, to in-service (IS step 17 a.). Or, change the state of the downstream TIC VT1.5, if it was incorrectly changed to the in-service state, to out-of-service (step 17 b.). If the VT is carrying traffic, go to step 19.

a. To change the state of the DS1 to IS:

select <group> <port>↵

chgstate is.↵

y↵

where

<group>	is the group number of the DS1 (GR-303 or DS1 tandem): see “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.
<port>	is the port number of the DS1 facility: **1** to **14**.

The state of the DS1 facility changes to in-service (IS).

Repeat this step for each DS1 facility that has to be returned to in-service.

b. To change the state of the downstream VT1.5 to OOS, log in to the remote network element and enter the following commands:

fa tic < sts-1 # > ↵

where

<STS-1 #>	is the number of the STS-1 associated with UDLC or GR-303 traffic, or DS1 tandem.

vtselect < VT # > ↵

where

<VT #>	is the number of the VT reporting this alarm: **1** to **28**.

chgstate oos ↵

yes ↵

The TIC facility screen is updated with the new operating state in reverse video, and this alarm should clear.

—continued—

Fac TIC
VT Rx unequipped (continued)

Step	Action

18 Determine the state of this alarm:

If the alarm	Then
clears	end the procedure.
persists	go to step 19.

19 Perform a protection switch on the FCOT GR-303, DS1/VT mapper:

a. From the Network Element Status screen, display the DS1 protection switching screen:

pr;dtlprot ds1↵

The DS1 detailed protection switching screen appears.

b. Operate the manual switch:

manual op < group >↵
y↵

where

< group >	number of the DS1 group: see “Group and slot associations for DS1, DS3, STS-1, OC-3, and OC-12” on page 1-15.

When a manual switch is operated, the screen displays an asterisk (*****) in the `Manual` *column.*

If the alarm	Then
clears	go to step 20.
persists	go to step 21.

20 Replace the DS1/VT mapper from which service was switched in step 19, as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. End the procedure.

21 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Clearing an environmental alarm

This chapter describes how to clear environmental-class (Env) alarms. The alarms in this chapter appear alphabetically. The banner at the beginning of each alarm shows the alarm group and the text of the alarm. The procedure describes the cause of the alarm and the action needed to clear it.

Chapter contents

The following table organizes environmental (Env) alarms by alarm group as common equipment (CE) alarms. The table lists the alarms within the group and the page numbers for the alarm procedures.

Table 5-1
Env ANX alarms

Alarm	See
Remote environmental critical	page 5-3
Remote environmental major	page 5-3
Remote environmental minor	page 5-3

Table 5-2
Env CE alarms

Alarm	See
Fan 1 fail, Fan 2 fail, Fan 3 fail	page 5-4
Fan 1 fail, 800A	page 5-5
High bay temperature	page 5-7
High CE shelf temperature	page 5-10
Talk battery filter fail	page 5-13
Telemetry input 1-11	page 5-14
—continued—	

Table 5-2 (continued)
Env CE alarms

48V battery A CE supply fail	page 5-15
48V battery B CE supply fail	page 5-18
48V CDS breaker tripped ext bay	page 5-21
48V CDS breaker tripped main bay	page 5-22
48V CE, CU or TB CE breaker tripped main bay	page 5-23
—end—	

Env ANX
Remote environmental critical
Remote environmental major
Remote environmental minor

The following alarms are AccessNode Express environmental alarms.

- Remote environmental critical
- Remote environmental major
- Remote environmental minor

See *AccessNode Express Alarm and Trouble Clearing Procedures*, 323-3051-543, for information on AccessNode Express alarms and the appropriate alarm clearing procedures.

—end—

Env CE
Fan 1 fail,
Fan 2 fail,
Fan 3 fail

Probable cause

One of the three cooling modules in the NT4K18AA/BA cooling unit on the main bay (either 1, 2, or 3) is either missing or has failed or the 8-fan cooling unit has failed (Fan 1 fail indication only).

Impact

This is a minor, not service-affecting (m, nsa) alarm. If the condition persists, the equipment may overheat.

Action

Step	Action

Note: Temperature related alarms can take up to one minute to clear.

1 Is the red fail LED on the cooling module or 8-fan cooling unit illuminated?

If	Then
yes	go to step 2
no	go to step 3

2 Replace the defective cooling module or 8-fan cooling unit as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5.

If the alarm persists, go to step 4.

3 Determine if a cooling module (NT4K18AA/BA only) is missing.

If	Then
yes	insert the missing module
no	go to step 4

4 Verify that there are no obstructions blocking the airflow in either the intake or exhaust of the cooling units.

5 Check the cooling unit interface cable, that connects the cooling unit to the CUIF connector on the side interconnect left circuit pack, for secure connection and no damage. Reseat or replace if necessary. If the alarm persists, go to step 6.

6 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Env CE
Fan 1 fail, 800A

Probable cause

One of the three cooling modules in the cooling unit on an 800A cabinet (either 1, 2, or 3) is either missing or has failed. All fan alarms (1, 2, and 3) in an 800A cabinet are tied to the "Fan 1 fail" alarm.

Impact

This is a minor, not service-affecting (m, nsa) alarm. If the condition persists, the equipment may overheat.

Action

Step	Action
	Note: Temperature related alarms can take up to one minute to clear.
1	Is the red fail LED on the cooling module illuminated? There are two cooling modules in an 800A cabinet. One is located between CDS 3 and 4, the other is located between the CE shelf and the BIP.

If	Then
yes	go to step 2
no	go to step 3

2	Replace the defective cooling module as outlined in *Series 800A Outside Plant Cabinet Installation*, 323-3001-210. If the alarm persists, go to step 3.
3	Does this cabinet contain a heat exchanger roof?

If	Then
yes	go to step 4
no	go to step 11

4	Open the electronics compartment doors on the front of the cabinet.
5	Open the equipment bat frames and inspect the eight internal fans located at the top of the cabinet.
6	If a defective fan unit cannot be identified by inspection, disconnect each fan unit one at a time, until the defective unit is identified. *The alarm will extinguish when the defective fan unit is disconnected.* If no defective fan unit is identified, go to step 8.

—continued—

Env CE
Fan 1 fail, 800A (continued)

Step	Action
7	If a defective fan unit is identified, replace the unit as described in *Series 800A Outside Plant Cabinet Installation*, 323-3001-210. If the alarm persists, go to step 8.
8	Remove the heat exchanger roof cover by loosening the 10 1/4 turn fasteners and removing the four lifting eye bolts. This requires a can wrench (216 tool) with Harris insert part number 1066-001.
9	Inspect the 4 external fans located inside the heat exchanger roof. If a defective fan cannot be identified, disconnect each fan unit, one at a time until the defective unit is identified. *When the defective fan is identified, the alarm extinguishes.* If no defective fan unit is identified, go to step 11.
10	Replace the defective unit as described in *Series 800A Outside Plant Cabinet Installation*, 323-3001-210. If the alarm persists, go to step 14.
11	Open the electronics compartment doors on the front of the cabinet.
12	Open the equipment bay frames and inspect the 11 fan units located at the top of the cabinet. If a defective fan unit cannot be identified by inspection, disconnect each fan unit, one at a time until the defective unit is identified. *When the defective fan is identified, the alarm extinguishes.* If no defective fan unit is identified, go to step 14.
13	Replace the defective unit as described in *Series 800A Outside Plant Cabinet Installation*, 323-3001-210. If the alarm persists, go to step 14.
14	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Env CE
High bay temperature

Probable cause

An excessively high temperature is detected in the main bay or cabinet. The high temperature sensors indicate a temperature over 70°C (158°F) due to

- a defective cooling unit or fan
- clogged filters
- an excessively high central office temperature
- defective high temperature sensors

Note: It may take up to 15 seconds to raise this alarm.

High temperature heat sensors are employed in bay frames, modular business package (MBP) cabinets and Series 800A outside-plant cabinets to detect excessive equipment temperatures. If temperatures within a bay or cabinet exceed a preset high temperature threshold of 70°C (158°F), a critical alarm is generated.

In a bay frame configuration, there are two high temperature heat sensors located in each cooling module of the cooling unit.

In the Series 800A outside-plant cabinet, there is one high temperature heat sensor located in the roof module. For the S800A closed-loop heat exchanger roof assembly, the sensor is located on the underside of the mounting plate of the heat-exchanger roof, between the two rows of fans. For the S800A air induction roof assembly, the sensor is located on a metal flange that attaches to the exhaust fan assembly. For details, see the cabinet introduction chapter in *Series 800A Outside Plant Cabinet Description,* 323-3001-118.

In the MBP cabinet, there are two high temperature heat sensors located in the top cap module.

Impact

This is a critical, not service-affecting (C, nsa) alarm. If the condition persists, the equipment may overheat.

—continued—

Env CE
High bay temperature (continued)

Action

Step	Action
1	Verify that there are no obstructions blocking the fan intake or exhaust. ***Note:*** In the bay frame, the fans have louvers both underneath the cooling units, and to the rear. Ensure that both sets of louvers are free of obstructions.
2	Check for a `Fan 1/2/3 fail` alarm. ***Note:*** For details on listing alarms see “Displaying alarms” on page 1-2.

If there are	Then
fan alarms	Clear the alarms using the appropriate procedure in this document, then return to this procedure. Go to step 3.
no fan alarms	go to step 3

3 Wait one minute then determine if the `High bay temperature` alarm clears.

If the alarm	Then
clears	end the procedure
persists	go to step 4

4 Follow the procedure “High CE shelf temperature” on page 5-10, then return to this point.

If the High bay temperature alarm	Then
clears	end the procedure
persists	Determine if you are working on a bay frame or an MBP or S800A cabinet. If you are working on a bay frame, go to step 5. If you are working on an MBP or S800A, go to step 8.

—continued—

Env CE
High bay temperature (continued)

Step	Action
5	Remove one of the cooling modules (NT4K18AA/BA) and leave it out of the shelf for two minutes. For the 8-fan cooling unit open circuit breakers CU-1 and CU-2 on the BIP for two minutes. ***Note:*** For details, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
6	While the cooling module is removed, determine if the `High bay temperature` alarm clears.

If the alarm	Then
clears	the cooling module that you have removed or the 8-fan cooling unit is faulty. Replace this cooling module or the 8-fan cooling unit as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
persists	go to step 7

7	Re-insert the cooling module and repeat steps 5 and 6 for each cooling module in the cooling unit.
8	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Env CE
High CE shelf temperature

Probable cause

The temperature in the common-equipment (CE) shelf is excessively high.

Note: The maintenance interface card (MIC), which detects this condition waits for 15 seconds before raising the alarm. The actual sensor is on the MIC board.

Impact

This is a critical, not service-affecting (C, nsa) alarm. If the condition persists, the equipment may overheat.

Action

Note: temperature related alarms can take up to one minute to clear.

Step	Action
1	Check the equipment for abnormal environmental conditions such as excessive room temperature.

If the ambient room temperature is	Then
normal	go to step 3
too high	go to step 2

Step	Action
2	Take steps to lower the temperature. The alarm can take up to 1 minute to clear after correcting the room temperature. If the alarm does not clear after one minute, go to step 3.
3	Is the red fail LED on the cooling module or 8-fan cooling unit illuminated?

If	Then
yes	go to step 4
no	go to step 5

Step	Action
4	Replace the cooling module or 8-fan cooling unit as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

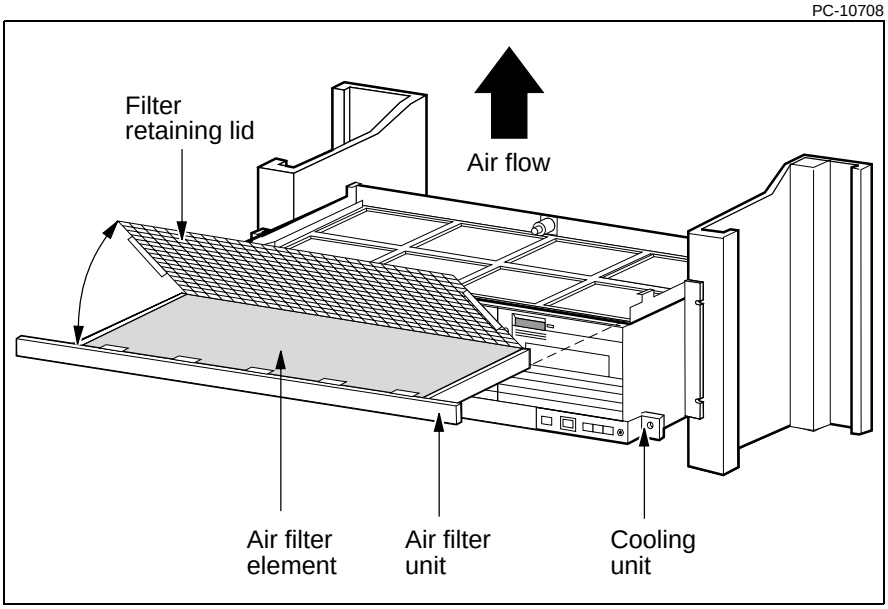
If	Then
clears	end the procedure
persists	go to step 5

—continued—

Env CE
High CE shelf temperature (continued)

Step	Action
5	Verify that there are no obstructions blocking the airflow on either the intake or exhaust of the cooling units.
6	Locate the air filter in the filter tray at the top of the cooling unit (NT4K18AA only) shelf. (The position of the cooling unit varies with the equipment configuration.)
7	Disengage the air filter unit from its locking mechanism by quickly pushing and releasing the front face of the air filter unit. Remove the air filter unit by pulling it outward.
8	Lift the filter retaining lid, and inspect the condition of the air filter, as shown following.

PC-10708



—continued—

Env CE
High CE shelf temperature (continued)

Step	Action

9 Is the air filter clean?

If	Then
yes	go to step 11
no	go to step 10

10 Replace the air filter and reinsert the filter tray into the shelf. Wait one minute for the alarm to clear.

If the alarm	Then
clears	end the procedure
persists	go to step 11

11 Clean the cooling unit grille of any dust buildup as outlined in *Routine Maintenance Procedures*, 323-3001-546, Volume 5C.

If the alarm	Then
clears	end the procedure
persists	go to step 12

12 Insert a temperature probe into the CE shelf to monitor the temperature. If the measured temperature does not exceed 70°C, then the MIC card may be giving a false indication. Replace the MIC, and see that the alarm clears.

13 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Env CE
Talk battery filter fail

Probable cause

The talk battery filter card failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Replace the talk battery filter card as outlined in *Module Replacement Procedures,* 323-3001-547, in *Maintenance,* Volume 5C.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Env CE
Telemetry input 1-11

Probable cause

One of 11 provisionable external parallel telemetry inputs has been activated by a condition that meets the user-provisioned criteria for an alarm.

Impact

Except for the following three telemetry input defaults, the severity of the telemetry alarms is provisionable, and the impact will vary according to the provisioned value:

- Input 1: “AC power fail,” minor not service-affecting (m, nsa)
- Input 2: “Low battery,” major, not service-affecting (M, nsa)
- Input 3: “Reserved for future use,” minor, not service-affecting (m, nsa)

Action

Because the 11 telemetry inputs are user-provisionable, there is no single procedure to clear this alarm. The procedure varies depending on provisioning of each input. Use the following procedure to obtain more details on this alarm.

Step	Action
1	From any screen display the alarm screen: **alarms**↵ *The list of active alarms appears.*
2	Display the detailed alarm screen for the telemetry input alarm: **dtlalms < alarm # >**↵ where < alarm # > is the number of the telemetry alarm that appears under the heading Alm on the alarm screen
3	Display the telemetry input alarm parameters: **portø**↵ *The screen displays the details of the telemetry alarm.*
4	Proceed according to the severity and details of the alarm.
5	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Env CE
48V battery A CE supply fail

Probable cause

There is a failure in the CE PWR A (common-equipment power A) feed from the Breaker Interface Panel (BIP) to the common-equipment power card.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action

1 Check the breaker interface panel (BIP) for a tripped circuit breaker labelled CE A for an NT4K14 BIP, A1, or A3, or A4 for an NT4K56 BIP (A1 if TBM shelf is located in position 1, A3 if TBM shelf is located in position 2, A4 if TBM shelf is located in position 3.

If the breaker is	Then
tripped	go to step 2
not tripped	go to step 3

2 Reset the breaker.

If the alarm	Then
clears	end the procedure here
persists	go to step 3

3 Ensure that the common-equipment power card and its modular connector are securely in place.

If the alarm	Then
clears	end the procedure here
persists	go to step 4

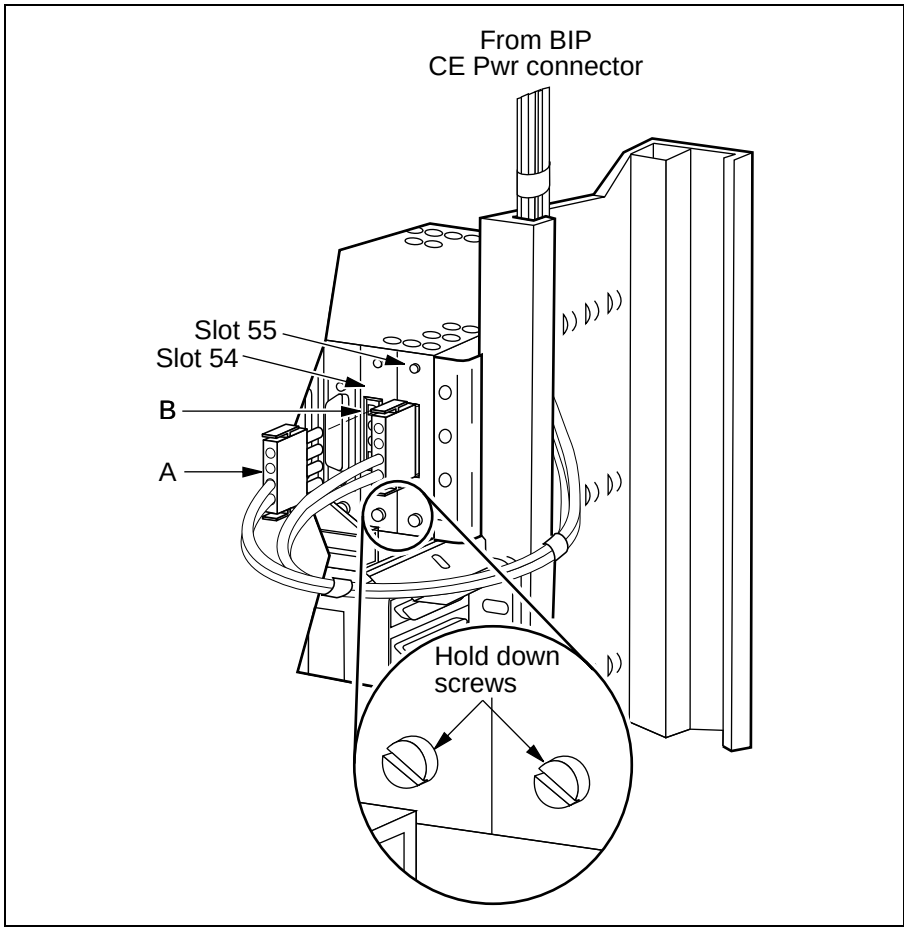
4 Disconnect the power cable from the common-equipment power card (slot 54), as shown in the following figure.

—continued—

Env CE
48V battery A CE supply fail (continued)

Step	Action

PC-11481



5 Connect a digital voltmeter across the power cable connector and measure the voltage.

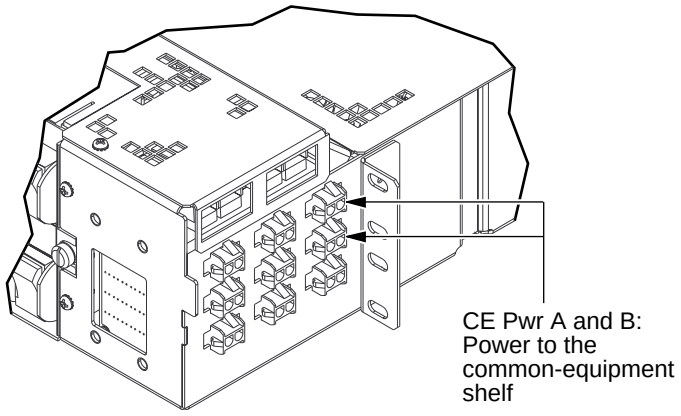
If the –48 volts	Then
is present	go to step 6
is not present and the common equipment shelf is an ABM	go to step 8
is not present and the common equipment shelf is a TBM	go to step 10

—continued—

Env CE
48V battery A CE supply fail (continued)

Step	Action
6	Examine the connector on the common-equipment power card for foreign matter. Reconnect the cable, wiggling it to ensure good contact (clean contacts if necessary). If the alarm clears, end the procedure here. If the alarm persists, go to step 7.
7	Replace the common-equipment power card, as described in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. Go to step 11.
8	Disconnect the common-equipment power cable from the side of the BIP.

PC-16513



Right side of BIP

Step	Action
9	Connect a digital voltmeter across the common-equipment shelf CE Pwr A connector and measure the voltage.

If the –48 volts	Then
is present	replace the CE power cable; end the procedure here
is not present	go to step 10

10	Verify the power cable between the dc power source and the BIP, or whether the dc power source is faulty. Repair as required.
11	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Env CE
48V battery B CE supply fail

Probable cause

There is a failure in the CE PWR B (common-equipment power B) feed from the Breaker Interface Panel (BIP) to the common-equipment power card.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Step	Action

1 Check the breaker interface panel (BIP) for a tripped circuit breaker labelled CE B for an NT4K14 BIP, B1, or B3, or B4 for an NT4K56 BIP (B1 if TBM shelf is located in position 1, B3 if TBM shelf is located in position 2, B4 if TBM shelf is located in position 3.

If the breaker is	Then
tripped	go to step 2
not tripped	go to step 3

2 Reset the breaker.

If the alarm	Then
clears	end the procedure
persists	go to step 3

3 Ensure that the common-equipment power card and its modular connector are securely in place.

If the alarm	Then
clears	end the procedure
persists	go to step 4

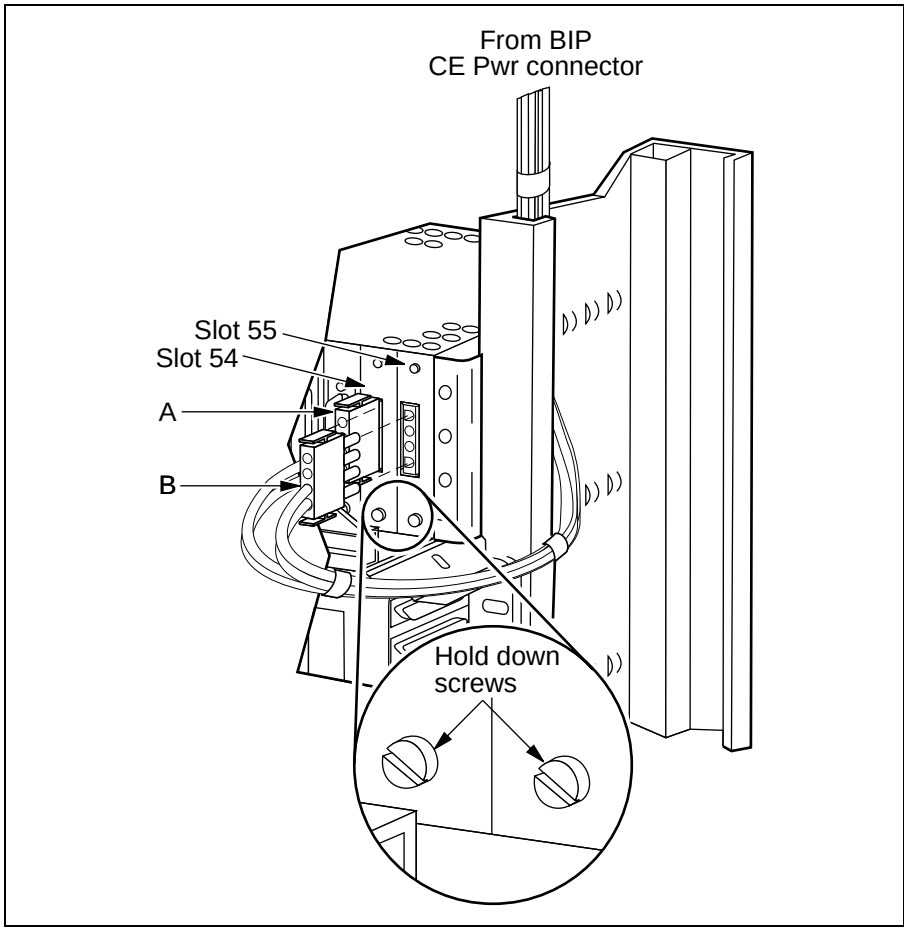
4 Disconnect the power cable from the common-equipment power card (slot 55), as shown in the following figure.

—continued—

Env CE
48V battery B CE supply fail (continued)

Step	Action

PC-11480



5 Connect a digital voltmeter across the power cable connector and measure the voltage.

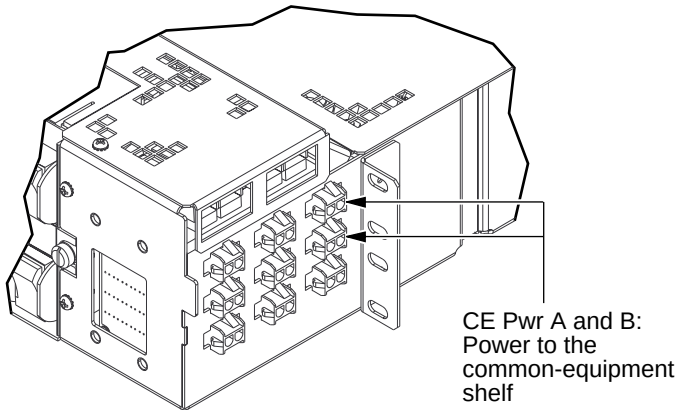
If the –48 volts	Then
is present	go to step 6
is not present and the common equipment shelf is an ABM	go to step 8
is not present and the common equipment shelf is a TBM	go to step 10

—continued—

Env CE
48V battery B CE supply fail (continued)

Step	Action
6	Examine the connector on the common-equipment power card for foreign matter. Reconnect the cable, wiggling it to ensure good contact (clean contacts if necessary). If the alarm clears, end the procedure here. If the alarm persists, go to step 7.
7	Replace the common-equipment power card, as described in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. Go to step 11.
8	Disconnect the common-equipment power cable from the side of the BIP.

PC-16511



Right side of BIP

Step	Action
9	Connect a digital voltmeter across the common-equipment shelf CE Pwr B connector and measure the voltage.

If the –48 volts	Then
is present	replace the CE power cable; end the procedure
is not present	go to step 10

10	Verify the power cable between the dc power source and the BIP, or whether the dc power source is faulty. Repair as required.
11	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Env CE
48V CDS breaker tripped ext bay

Probable cause

One of the copper distribution shelf (CDS) power breakers or CDS talk battery breakers is tripped on the breaker interface panel (BIP) of the extension bay.

Impact

This is a major, not service-affecting (M, nsa) alarm.

Action

Reset the tripped breaker on the extension bay BIP. These breakers are labeled Power CDS1 through Power CDS7 and Talk Battery CDS1 through Talk Battery CDS7.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Env CE
48V CDS breaker tripped main bay

Probable cause

One of the CDS Power, or CDS Talk Battery breakers is tripped on the Breaker Interface Panel (BIP) of the main bay.

Impact

This is a major, not service-affecting (M, nsa) alarm.

Action

Reset the tripped CDS Power, or CDS Talk Battery breaker on the main bay BIP. These breakers are labeled “Power CDS1” through “Power CDS 7", and “Talk Battery CDS1” through “Talk Battery CDS7”.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Env CE
48V CE, CU or TB CE breaker tripped main bay

Probable cause

One of the breakers is tripped on the Breaker Interface Panel (BIP) of the main bay.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Action

Reset the tripped breaker on the main bay BIP.

If you cannot successfully complete this procedure, contact your next level of support.

—end—

Troubleshooting PGTC/MTA

Use this chapter to troubleshoot problems with the pair gain test controller/metallic test access (PGTC/MTA) card.

Chapter contents

In the following table, look up the task you are required to perform, and proceed to the page specified.

Topic	See
Troubleshooting PGTC/MTA access failures	page 6-2

Troubleshooting PGTC/MTA access failures

Use Table 6-1 to troubleshoot PGTC/MTA access failures. If you experience test access failure to a line card from a PGTC or MTA testing system, try one or more of the suggestions in the table to correct the problem.

If you cannot successfully troubleshoot the failure, contact your next level of support.

Note: Acronyms in Table 6-1 are defined in Table 6-2.

Table 6-1
Troubleshooting PGTCM/MTA access failures

	Condition		Possible cause	Corrective action
1	System does not respond to Test bypass initiate signal	a.	The PGTC/MTA has not been provisioned from the OPC	Provision with the PGTC/MTA Provisioning Manager (Use Procedure).
		b.	The FCOT line card state is not in-service—Normal (IS-NR), might be failed, OOS, unequipped, or parent equipment unavailable	Verify the line card status on the LC Equipment screen.
		c.	The TAC state is not in-service—Normal (IS-NR), might be failed, OOS, or unequipped	Verify the TAC status in the TAC Equipment screen.
		d.	Test access (metallic jack or 0TLP jack) is already active on the FCOT line card	Verify the line card status on the LC Equip screen. Remove jack access if it is present.
		e.	FCOT is a rebooting or restarting	Wait for reboot or restart to end.
		f.	Line cards are provisioned other than POTS, COIN, or UVG (**Note**: FX is not supported)	PGTC/MTA is only permitted on POTS, COIN, or UVG provisioned lines.
		g.	Test initiate signal is not within limits	Check the testing system. See TR-465 for PGTC test initiate requirements.

—continued—

Table 6-1
Troubleshooting PGTCM/MTA access failures (continued)

	Condition		Possible cause	Corrective action
1	System does not respond to Test bypass initiate signal (continued)	h.	Test initiate signal was applied for less than one second (Urban MTA only) or less than five seconds for coin	For URBAN MTA, apply test initiate for the proper duration.
2	Urban MTA: reorder tone is returned	a.	The required I/O cards are not present (see Note 3)	Verify I/O cards status on the TAC Equipment screen.
		b.	The RFT TAC state is not in-service—normal (IS-NR), might be failed, OOS, or unequipped	Verify TAC status on the TAC Equipment screen.
		c.	The RFT MTAC in the line drawer with the line card under test is not in-service—normal (IS-NR), might be failed, OOS, or unequipped	Verify MTAC status on the MTAC Equipment screen.
		d.	The FCOT MTAC in the line drawer containing the line card under test is not in the In-service—Normal (IS-NR) state, might be failed, OOS, or unequipped	Verify MTAC status in the MTAC Equipment screen
3	Urban MTA: busy tone is returned	a.	The test resources are busy at either the FCOT or RFT (see Note 1)	
		b.	The test bypass pair inhibit lead has been grounded by other testing activity. Indicates that TBP is busy.	Check for ground on the inhibit lead of the TBP I/O card (if equipped). If not grounded, and carrier continues to return busy tone, replace the TBP I/O and/or TAC card.
4	PGTC: TMAJ is returned by the carrier	a.	A major or critical alarm exists on the FCOT or RFT.	Clear the alarms.

—continued—

Table 6-1
Troubleshooting PGTCM/MTA access failures (continued)

	Condition		Possible cause	Corrective action
5	PGTC: SEZBY is returned by the carrier	a.	The test bypass pair inhibit lead has been grounded by other testing activity, indicating that the TBP is busy	Check for ground on inhibit lead. If not grounded, and carrier continues to return SEZBY, replace the TBP I/O and/or TAC card.
6	PGTC: the sequence is aborted before the SLEEVE condition is asserted by the carrier	a.	Metallic test access at the RFT has failed due to test resources busy (see Note 1)	
		b.	RFT TAC is not In-service-Normal (IS-NR), might be failed, OOS, or unequipped	Verify TAC status on the TAC Equipment screen
		c.	RFT MTAC in the line drawer with the line card under test is not in-service-normal (IS-NR) might be failed, OOS, or unequipped	Verify MTAC status on the MTAC Equipment screen.
		d.	Required I/O cards are not present (see Note 3)	Verify I/O card status on the screen.
7	Urban MTA: request for teardown or results reporting ignored	a.	Test report or teardown signal is not of correct polarity	Verify correct polarity is selected with the PGTC/MTA provisioning tool on the OPC.
—end—				

Note 1: Test Resources busy can indicate any of the following:

- The drawer test bus of the line drawer with the line card under test is busy because of the following:
  - — another line card in the drawer is undergoing line card diagnostics
  - — another line card in the drawer has metallic jack access active
- System test buses are unavailable because of MTAC circuit pack diagnostics
- System test buses are unavailable because of multiple maintenance activities; for example, metallic jack access on test bus 2 and line card diagnostics on test bus 1

Note 2: For either PGTC or Urban MTA, the following RFT equipment must be in-service:

- TAC
- MTAC in the drawer of the line card to be tested
- line termination of the line card to be tested
- TAP I/O card

Additionally, for Urban MTA, the following FCOT equipment must be in-service:

- TAC
- MTAC in the drawer of the line card to be tested
- line termination of the line card to be tested
- PGTC/MTA I/O card
- TBP I/O card

PGTC requires the same FCOT equipment to be in-service as the Urban MTA, but the MTAC is not required.

Note 3: The provisioning of the PGTC/MTA determines the required TAC I/O cards:

- The PGTC/MTA I/O card at the FCOT and the TAP I/O card at the RFT are always required.
- The FCOT TBP I/O card is required if the TBP Card installed at FCOT button is selected for PGTC provisioning.
- The FCOT TBP I/O card is always required for Urban MTA.

Table 6-2
Description of acronyms

Acronym	Description
FCOT	fiber central office terminal
FX	foreign exchange
MTA	metallic text access
OOS	out of service
OPC	operations controller
RFT	remote fiber terminal
TAC	test access card
UVG	universal voice grade

Interpreting an LED or lamp

This chapter explains the meaning of the status LEDs on AccessNode circuit packs, cards, and modules, and the lamps and LEDs on the breaker interface panel.

Note: Do not troubleshoot circuit packs from the LEDs. Always troubleshoot an alarm condition from the network element user interface. See Chapter 1 for directions to clear alarms from the network element user interface.

Chapter contents

In the following list, look up the name and product equipment code for the circuit pack in question, then proceed to the page specified.

Equipment	See
Line drawer (NT4K21)	page 7-7
Processor circuit pack (NT4K52)	page 7-8
Maintenance interface circuit pack (NT4K53)	page 7-9
Test access card (NT4K54)	page 7-11
Access interface card (NT4K55)	page 7-12
Transport interface card (NT4K56)	page 7-13
Integrated remote test unit (NT4K57)	page 7-14
Copper distribution shelf power (NT4K62AA)	page 7-15
Epsilon 2-wire station line card (NT4K65AA)	page 7-16
Omega 2-wire station line card (NT4K67AB)	page 7-17
Omega 2-wire office line card (NT4K68AA)	page 7-18
Omega 4-wire line card (NT4K69AA)	page 7-19
Narrowband line interface card (NT4K70AA)	page 7-20
Metallic test access card (NT4K73AA)	page 7-21
Metallic test access card (NT4K73CA)	page 7-22
Omega 6- 8-wire line card (NT4K77AA)	page 7-23
OC-3 (Optical carrier level 3) (NT7E01)	page 7-24
OC-12 (Optical carrier level 12) (NT7E02)	page 7-25
OC12 optical interface circuit pack (NT7E05)	page 7-26
DS1/VT mapper (NT7E04)	page 7-27
DS3/STS mapper (NT7E08)	page 7-28
STS-1 interface card (NT7E09)	page 7-29
OPC (Operations Controller) (NT7E24)	page 7-30
—continued—	

Equipment	**See**
External synchronization interface (NT7E27)	page 7-31
OPC (Operations Controller) tape drive unit	page 7-32
Interpreting breaker interface panel (BIP) LEDs	page 7-34
—end—	

Status of all active and fail LEDs

Table 7-1 shows how to interpret the status of the green Active LED and the red Fail LED for each *in-service* module, circuit pack, or card in the AccessNode shelves.

> ***Note:*** During a processor card SWACT, the green active LED on working DS1/VT mappers and DS3/STS mappers goes out for approximately 20 seconds. The DS1/DS3 mappers are fully functional during this 20 second interval and there is no loss of traffic.

Table 7-1
Interpreting status LEDs for in-service modules, circuit packs and cards

Module, circuit pack, or card	Active LED (green)	Fail LED (red)
Processor (active)	ON	OFF (1)
Processor (standby)	OFF	OFF
MIC	ON	OFF (1)
OPC	ON	OFF
TAC	ON	OFF
OC-12 (active)	ON	OFF
OC-12 (standby)	OFF	OFF
DS1	ON	OFF
DS1 (protection)	OFF (2)	OFF
DS3	ON	OFF
DS3 (protection)	OFF (2)	OFF
STS-1	ON	OFF
STS-1 (protection)	OFF (2)	OFF
ESI (active)	ON	OFF
ESI (standby)	OFF	OFF
TIC (primary)	ON	OFF
TIC (secondary)	ON	OFF
AIC (A)	ON	OFF
AIC (B)	ON	OFF
LIC (primary)	ON	OFF
LIC (secondary)	OFF (3)	OFF
Line card	n/a	OFF
MTAC	n/a	OFF

—continued—

Table 7-1 (continued)
Interpreting status LEDs for in-service modules, circuit packs and cards

IRTU	ON	OFF
CDSP	n/a	OFF
Note (1): ON, if subset of card has failed (In-service, partial fail) Note (2): ON. if DS1, DS3, STS-1 protection card is providing protection Note (3): ON, if secondary LIC is data active		
—end—		

Table 7-2 shows how to interpret the green Active LED and the red Fail LED for an *out-of-service* module, circuit pack or card in the AccessNode shelves.

Table 7-2
Interpreting status LEDs for out-of-service modules, circuit packs and cards

Module, circuit pack, or card	**Active LED (green)**	**Fail LED (red)**
Processor	OFF	OFF
MIC	OFF	OFF
OPC (1)	ON	OFF
TAC	OFF	OFF
OC-12	OFF	OFF
DS1, DS3, STS-1	OFF	OFF
ESI	OFF	OFF
TIC	OFF	OFF
AIC	OFF	OFF
LIC (2)	OFF	OFF
Line card	n/a	OFF
MTAC	n/a	OFF
CDSP (2)	n/a	OFF
IRTU	OFF	OFF
Note (1): Out-of-service OPC cannot be removed until OPC shutdown is performed. Note (2): Red LED is ON if there is a failure on the card detected by hardware.		

Table 7-3 shows how to interpret the green Active LED and the red Fail LED for a *failed* module, circuit pack or card in the AccessNode shelves.

Table 7-3
Interpreting status LEDs for failed modules, circuit packs and cards

Module, circuit pack, or card	Active LED (green)	Fail LED (red)
Processor	OFF	ON
MIC	OFF	ON
OPC	OFF	ON
TAC	OFF	ON
OC-12	OFF	ON
DS1, DS3, STS-1	OFF	ON
ESI	OFF	ON
TIC	OFF	ON
AIC	OFF	ON
LIC	OFF	ON
Line card	n/a	ON
MTAC	n/a	ON
CDSP	n/a	ON
IRTU	OFF	ON

Line drawer (NT4K21)
Fail (red)

Probable cause

The red LED on the line drawer can light for any of the following reasons:

- the MTAC is faulty
- one or more of the line cards is faulty
- one or more of the line card slots is faulty

Note: If the drawer's red LED is on, and none of the circuit packs indicate a fail condition, there is a possibility of a line card mismatch alarm related to the non-primary slot of a 4-wire or 6/8-wire line card. Check all slots associated with a multi-slot line card.

For example, if a 6/8-wire line card is installed in slots 1, 2, 3, and 4, the primary slot is slot 2. If a 2-wire card is inserted in slot 4, a mismatch condition exists, but does not alarm the primary slot, which is slot 2. This condition will light the red LED on the drawer.

Impact

Because there are a number of alarm conditions that can cause the red fail LED to light, the impact on service can not be determined by the LED. Display a list of alarms for the network element and look for equipment alarms related to the equipment housed in the line drawer. Look up the reason for the alarm in this document, and proceed as instructed.

Processor circuit pack (NT4K52)
Fail (red)

Probable cause

There is a problem associated with the processor circuit pack.

Impact

Because there are a number of alarm conditions that can cause the red fail LED to light, the impact on service can not be determined by the LED. Display a list of alarms for the network element and look for Eqp Proc alarms. Look up the reason for the alarm in this document, and proceed as instructed.

Note: On insertion of an inactive processor card, if the red fail LED lights on both processors, replace the newly inserted processor. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

Maintenance interface circuit pack (NT4K53)

CU (yellow)

Probable cause

This LED is not currently being used.

Impact

None.

Fail (red)

Probable cause

The circuit pack has failed.

Impact

Although this alarm does not affect service, it is best to take corrective action immediately. Display a list of alarms for the network element and look for *Eqp MIC* alarms. Look up the reason for the alarm in this document, and proceed as instructed.

This alarm may cause a corresponding alarm to be raised on the processor circuit pack: either *C-bus-A fail, C-bus-B fail, Degraded master CBIC-A,* or *Degraded master CBIC-B*. Take corrective action for the MIC first, then if the processor alarms persist, correct the fault for the processor.

Init (yellow)

Probable cause

The system is initializing the software (downloading the processor card).

Impact

Not applicable.

LckOut (yellow)

Probable cause

A DS1, DS3, STS-1, ESI or OC-12 protection lockout is in effect.

Impact

Traffic cannot be switched to the locked-out card.

LoopBk (yellow)

Probable cause

A DS1, DS3, or STS-1 loopback is set for a DS1, DS3, or STS-1 facility.

Impact

The DS1, DS3, or STS-1 facility is out of service for the duration of the loopback.

Temp (red)

Probable cause

The MIC has detected a high shelf temperature.

Impact

Display a list of alarms for the network element and look for *Eqp MIC* alarms. Look up the reason for the alarm in this document, and proceed as instructed.

TestFail (red)

Probable cause

Either an OC-3, OC-12, DS1, DS3, STS-1 or processor failed the exerciser test. To find out which card failed, perform a manual exerciser test, then check the EQP logs. For details, see “Manually testing the protection groups on a shelf” on page 8-2.

Impact

This is a minor, not service-affecting (m, nsa) alarm. Service cannot be switched to the standby OC-3, OC-12, DS1, DS3, or STS-1 in the event of a service-affecting alarm.

TestRun (yellow)

Probable cause

An OC-3, OC-12, DS1, DS3, STS-1 or processor exerciser test is in progress.

Impact

The exerciser test has no effect on service.

Test access card (NT4K54)
Fail (red)

Probable cause

There is a problem with the test access card or one of its associated cards, such as the PGTC, TBP, or TAP.

> ***Note:*** If the system is operational and an AIC, TIC, OC-3, or OC-12 card is removed, the red fail LED on the TAC may light momentarily with no alarm generated. However, a TAC fault log (TAC300) will be raised and cleared. When this condition occurs, any test sessions in progress, such as a PGTC test, will be dropped. The test session will have to be reinitiated.

Impact

Because there are a number of alarm conditions that cause the red fail LED to light, the impact on service can not be determined by the red LED. Display a list of alarms for the network element and look for *Eqp TAC*, or *Eqp MTAC* alarms. Look up the reason for the alarm in this document, and proceed as instructed.

Access interface card (NT4K55)
Fail (red)

Probable cause

The access interface card has failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Transport interface card (NT4K56)
Fail (red)

Probable cause

The transport interface card has failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Integrated remote test unit (NT4K57)
Fail (red)

Probable cause

The integrated remote test unit has failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Copper distribution shelf power (NT4K62AA)
Fail (red)

Probable cause

The copper-distribution shelf power card has failed.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Epsilon 2-wire station line card (NT4K65AA)
Fail (red)

Probable cause

The line card has failed.

Impact

This is a minor, service-affecting (m, SA) alarm.

The associated 2-wire line has lost service.

For details on troubleshooting a failed Epsilon 2-wire station line card, see “Line card fail” on page 3-170.

If the state of the line card is Mism, the card is seated in a slot that is provisioned for 4 or 6/8 wire service. Change the provisioning or move the card to a slot provisioned for 2-wire service.

If the state of the line card is not Mism, replace the line card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

Omega 2-wire station line card (NT4K67AB)
Fail (red)

Probable cause

The line card has failed, or does not support the provisioned service.

Impact

This is a minor, service-affecting (m, SA) alarm.

The associated 2-wire line has lost service.

If the state of the line card is Mism, the card is seated in a slot that is provisioned for 4 or 6/8 wire service. Change the provisioning or move the card to a slot provisioned for 2-wire service.

If the state of the line card is not Mism, replace the line card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

Omega 2-wire office line card (NT4K68AA)
Fail (red)

Probable cause

The line card has failed, or does not support the provisioned service.

Impact

This is a minor, service-affecting (m, SA) alarm.

The associated 2-wire line has lost service.

If the state of the line card is Mism, the card is seated in a slot that is provisioned for 4 or 6/8 wire service. Change the provisioning or move the card to a slot provisioned for 2-wire service.

If the state of the line card is not Mism, replace the line card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

Omega 4-wire line card (NT4K69AA)
Fail (red)

Probable cause

The line card has failed, or does not support the provisioned service.

Impact

This is a minor, service-affecting (m, SA) alarm.

The associated 4-wire line has lost service.

If the state of the line card is Mism, the card is seated in a slot that is provisioned for 2 or 6/8 wire service. Change the provisioning or move the card to a slot provisioned for 4-wire service.

If the state of the line card is not Mism, replace the line card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

Narrowband line interface card (NT4K70AA)
Fail (red)

Probable cause

The narrowband line interface card failed or an associated AIC or TIC card has failed or has been taken out of service.

Impact

In an unprotected configuration, this is a major, service-affecting (M, SA) alarm.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

Metallic test access card (NT4K73AA)
Fail (red)

Probable cause

The metallic test access card has failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Metallic test access card (NT4K73CA)
Fail (red continuous or red blinking)

Probable cause

Continuous LED - Card fault detected in the copper-distribution shelf drawer.

Blinking LED - Loss of Talk Battery is detected in the copper-distribution shelf drawer.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

Omega 6- 8-wire line card (NT4K77AA)
Fail (red)

Probable cause

The line card has failed, or does not support the provisioned service.

Impact

This is a minor, service-affecting (m, SA) alarm.

The 6-wire or 8-wire line has lost service.

If the state of the line card is Mism, the card is seated in a slot provisioned for 2- or 4-wire service. Change the provisioning or move the card to a slot provisioned for 6- 8-wire service.

If the state is not Mism, diagnose the card (for details see “Performing a manual diagnostic test” on page 8-10). If the diagnostic fails, replace the line card as outlined in *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

OC-3 (Optical carrier level 3) (NT7E01)

Fail (red)

Probable cause

The circuit pack has failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm. Traffic associated with the OC-3 is lost.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

LOS (yellow)

Probable cause

There is no longer an optical signal being received.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm. Traffic associated with the OC-3 is lost.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

> ***Note:*** When an optical facility is taken out of service, the status of the loss of signal (LOS) LED becomes frozen, and will not reflect an actual loss of signal (if one occurs). When the optical facility is placed back in service, the LOS LED correctly indicates the current state of the optical facility.

OC-12 (Optical carrier level 12) (NT7E02)

Fail (red)

Probable cause

The circuit pack has failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm. Traffic associated with the OC-12 is lost.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

LOS (yellow)

Probable cause

There is no longer an optical signal being received.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm. Traffic associated with the OC-12 is lost.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

> ***Note:*** When an optical facility is taken out of service, the status of the loss of signal (LOS) LED becomes frozen, and will not reflect an actual loss of signal (if one occurs). When the optical facility is placed back in service, the LOS LED correctly indicates the current state of the optical facility.

OC12 optical interface circuit pack (NT7E05)

Fail (red)

Probable cause

The following are the probable causes of a red Fail LED on an optical interface circuit pack:

- the laser has failed or a circuit pack component has failed
- parity errors have been detected on the bus between a DS3STS mapper circuit pack or STS1 electrical interface and the optical interface

Impact

Upon detection of the failure, a high-speed switch occurs and causes a traffic hit of no more than 60ms.

LOS (yellow)

Probable cause

The following are the probable causes of a yellow LOS LED on an optical interface circuit pack:

- no optical signal is present at the optical interface (for example, due to a fiber cut or transmitter failure
- the received optical power is low
- the connector of the optical interface is dirty
- the mini-variable optical attenuator (mVOA) is malfunctioning
- the fiber optics patchcord is damaged

Impact

Upon detection of the failure, a high-speed switch occurs and causes a traffic hit of no more than 60ms.

Note: When this interface circuit pack is installed in a protected configuration, if the facility of one of the circuit packs which make up the protection pair is placed out of service, the LOS LED on both circuit packs is disabled, and cannot indicate a loss of signal should one occur. However, the facility Rx loss of signal alarm would still be raised.

DS1/VT mapper (NT7E04)
Fail (red)

Probable cause

The DS1/VT mapper circuit pack has failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm. Traffic associated with the DS1/VT mapper is lost.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

DS3/STS mapper (NT7E08)
Fail (red)

Probable cause

The DS3/STS mapper circuit pack has failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm. Traffic associated with the DS3/STS mapper is lost.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

STS-1 interface card (NT7E09)
Fail (red)

Probable cause

The STS-1 interface card has failed.

Impact

In an unprotected configuration, this is a critical, service-affecting (C, SA) alarm. Traffic associated with the STS-1 interface card is lost.

In a protected configuration, this is a minor, not service-affecting (m, nsa) alarm.

OPC (Operations Controller) (NT7E24)

Unit fail (red)

Probable cause

The OPC module has failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm; however, this failure does prevent personnel in a surveillance center from remotely gathering alarm information related to the network elements that are controlled by the failed OPC.

ELAN Fail (yellow)

Probable cause

There is a loss of Ethernet signal between the OPC module and the OPC X-terminal or workstation, or the Ethernet is currently not enabled.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

CNET Fail (yellow)

Probable cause

The OPC control network failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm.

External synchronization interface (NT7E27)
Fail (red)

Probable cause

The circuit pack has failed.

Impact

This is a minor, not service-affecting (m, nsa) alarm. External synchronization is switched to the protection external synchronization interface.

OPC (Operations Controller) tape drive unit

Note: The red and green LED indicators on the tape drive do not conform to FiberWorld standards. For example, the red LED does not necessarily indicate a failure.

Tape drive hardware status (red)

This indicator provides the status of the tape drive hardware.

Status	Probable cause	Action to take
OFF	no tape activity	none
ON	tape drive is reading or writing a tape without problems (this indication may be confused with flashing. The irregular timing of the on/off cycle will discriminate this condition)	none
FLASHING RAPIDLY	a hardware fault occurred, or moisture was detected	This condition may be temporary in the case of moisture. If it does not change within an hour, replace the tape drive.

Tape Drive Activity Status (green)

This indicator monitors transient errors and special purpose uses of the tape drive.

Status	Probable cause	Action to take
OFF	no tape activity; no tape in drive	none
ON	a tape is inserted in the drive and any transient errors occurring are below the predefined error threshold	none
FLASHING SLOWLY (in sync with the Red LED)	a prerecorded audio cassette is inserted and being played automatically. This tape drive capability is not currently used by the OPC and should not occur	Try the following steps until the fault clears: 1) remove the tape and reinsert it 2) use another tape 3) replace the tape drive
FLASHING SLOWLY	a tape is inserted in the drive and the number of transient errors has exceeded the predefined error threshold. This is a warning indication that tape reading and writing capability is deteriorating	Try the following steps until the fault clears: 1) try a new tape 2) clean the tape heads, using a Sony DDS DG-5CL cleaning cassette. The drive will eject this cassette after about 10 seconds 3) check for drive overheating 4) replace the tape drive
FLASHING RAPIDLY	the drive could not read/write a tape. This is an error indication that the current operation has failed	Try the following steps until the fault clears: 1) try a new tape 2) clean the tape heads, using a Sony DDS DG-5CL cleaning cassette. The drive will eject this cassette after about 10 seconds 3) check for drive overheating 4) replace the tape drive

Interpreting breaker interface panel (BIP) LEDs

This section explains the breaker interface panel (BIP) indicators.

ABM BIP indicators

The following visual indicators are located on the front of the NT4K14AB/BA BIP:

- Green power indicator. It is always lit when there is power to the system.
- Red critical alarm indicator. It is lit whenever a critical alarm exists.
- Red major alarm indicator. It is lit whenever a major alarm exists.
- Yellow minor alarm indicator. It is lit whenever a minor alarm exists.
- Red breaker-trip indicator. It is lit whenever any breaker is tripped or switched to the open position.
- Red fail indicators. From left to right on the TBF card:
  - — Red alarm relay indicator. It is lit when alarm relay card has failed or has lost power.
  - — Red TBF Alarm LED. It is lit when one or more fuses on the TBF card are blown.
  - — Red feed fail LED. It is lit when one of the power feeds on the left or the right side of the BIP are disabled.

  Note: In the non-redundant mode of operation this alarm is disabled by removing jumpers from connectors P# and P4 on the Alarm Relay card.

TBM BIP indicators

The following visual indicators are located on the front of the NT7E56 BIP:

Note: If the NT7E56 BIP is equipped with alarm indicator lamps rather than LEDs, and if one of those lamps is burned out, then the BIP alarm lamps will indicate a minor alarm until the lamp is replaced.

- Power indicator. It is white and is always lit when there is power to the frame.
- Critical alarm indicator. It is red, and is lit whenever a critical alarm exists.
- Major alarm indicator. It is red, and is lit whenever a major alarm exists.
- Minor alarm indicator. It is yellow, and is lit whenever a minor alarm exists.
- Breaker-trip indicator. It is red, and is lit whenever any breaker is tripped or switched to the open position.
- ACO indicator. It is green, and is lit whenever a cutoff of audible alarms is in effect.

Performing diagnostic tests

This chapter describes how to test AccessNode equipment and facilities and set up DS1 and DS3 facility loopbacks.

Chapter contents

This chapter includes the following topics:

Topic	See
Manually testing the protection groups on a shelf	page 8-2
Manually exercising the processor	page 8-4
Performing a lamp test from the NEUI	page 8-6
Performing a lamp test using the ACO/LAMP TEST button	page 8-8
Performing a manual diagnostic test	page 8-10
Setting or releasing a loopback on a DS1 or DS3 facility	page 8-14
Manually switching processor activity from active to standby	page 8-17
Manually restarting the processor	page 8-19
Manually restarting the shelf	page 8-23
Resetting a line card	page 8-26
Diagnosing failed CDS circuit packs	page 8-28
Generating alarms for testing purposes	page 8-32

For details on testing line cards see *Line Card Testing Procedures,* 323-3001-316, in *Operations, Administration, and Provisioning,* Volume 4B.

Procedure 8-1
Manually testing the protection groups on a shelf

Use this procedure to manually test OC-3, OC-12, DS1, and DS3 protection paths on a shelf, without affecting service. The exerciser tests the condition of each protection path to ensure that there are no failures that would otherwise not be detected until a protection switch occurred. This procedure is for a manual exerciser. However, the exerciser can be run automatically by scheduling it as a network event. Refer to *System Administration Procedures*, 323-3001-302, in *Operations, Administration, and Provisioning,* Volume 4A, for details.

This procedure uses the shelf exercise command.

Requirements

The exerciser does not perform a test if equipment is locked out, out of service, deleted, or unequipped. There must not be an active protection switch in effect when performing this test. For an OC-3/OC-12 exercise test, Rx traffic must be on G1.

Action

Step	Action
1	From the Network Element Status screen, display the equipment shelf screen: **eq sh**↵ *The equipment shelf screen appears.*
2	Run the exercise test: **exercise**↵ *The system displays the following message:* `The shelf exerciser has been initiated. Please refer to EQP608 logs for results.` The results of the test are output to equipment (EQP) log reports.
3	To view the log report, display the Log Utility screen: **admin nep;logs**↵ *The log utility screen appears.* ***Note:*** The command **logutil** can also be used to access the Log Utility screen.

—continued—

Procedure 8-1 (continued)
Manually testing the protection groups on a shelf

Step	Action
4	Display the last EQP log generated: **open eqp** ↵ If the last EQP log is not the EQP608 log, type **back**↵ until the EQP608 log appears. Each log report is explained in *Log Report Manual*, 323-3001-840, in *Maintenance*, Volume 5B.
5	Return to the Network Element Status screen: **quit**↵
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Procedure 8-2
Manually exercising the processor

Use this procedure to manually exercise (test) the inactive processor in a duplex configuration.

Requirements

Before manually exercising the inactive processor in a duplex configuration, both processors must be in-service normal (IS-NR).

The routine exercise must be enabled (on). If not enabled, use the command RexEna on the Proc equipment screen, to toggle the value from off to on.

Action

Step	Action
1	From the network element status screen, display the processor equipment screen: **eq proc <group>**↵ where <group> processor group number: **a** or **b** *The processor equipment screen appears.*
2	Check that the state of the active and redundant processor are IS.

If both processors are	Then
not in service (IS)	do not perform this test
in service (IS)	go to step 3

3	Perform the exercise test: **exercise**↵ *The results of the exercise test are reported in the EQP612 log report.*
4	To view the log report, display the Log Utility screen: **admin nep;logs**↵ *The log utility screen appears.* ***Note:*** The command **logutil** can also be used to access the Log Utility screen.

—continued—

Procedure 8-2 (continued)
Manually exercising the processor

Step	Action
5	Display the last EQP log generated: **open eqp** ↵ If the last EQP log is not the EQP612 log, type **back**↵ until the EQP612 log appears. Each log report is explained in *Log Report Manual*, 323-3001-840, in *Maintenance*, Volume 5B.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Procedure 8-3
Performing a lamp test from the NEUI

Use this procedure to test for defective lamps on the AccessNode equipment, by entering commands at the network element user interface (NEUI). During a lamp test from the NEUI, all functional lamps light for 30 seconds.

When a lamp test is performed on an access bandwidth manager (ABM) shelf, all lamps on the BIP and on the shelf circuit packs are tested. When a lamp test is performed on the transport bandwidth manager (TBM) shelf, only the circuit pack LEDs are tested, and not the lamps on the TBM BIP. To test the lamps on the TBM BIP, see "Performing a lamp test using the ACO/LAMP TEST button" on page 8-8.

> ***Note:*** The "Active" LED on the standby processor will not light if a restart is in progress, or if communication to the standby processor is down. The "Active" LED on the standby processor may turn off before other LEDs, if the active processor undergoes a restart, or may turn off after other LEDs, if the standby processor undergoes a restart during the lamp test.

Requirements

Read the commands conventions described in *Network Element User Interface Description*, 323-3001-300, in *Operations, Administration, and Provisioning*, Volume 4A.

Action

Step	Action
1	From the Network Element Status screen, display the equipment shelf screen: **eq sh** ↵ *The equipment shelf screen appears.*

—continued—

Procedure 8-3 (continued)
Performing a lamp test from the NEUI

Step	Action
2	Perform the lamp test: **lamptest** ↵ *For ABM shelves, the lamps on the circuit packs and the lamps on the BIP light for 30 seconds.* *For TBM shelves, only the circuit pack lamps light for 30 seconds. The BIP lamps do not light.* If a circuit pack LED does not light during the test, replace the circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C. If an ABM BIP lamp does not light during the test, replace the lamp. See *Routine Maintenance Procedures*, 323-3001-546, in *Maintenance*, Volume 5C. For BIPs with an LED card, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.
3	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Procedure 8-4
Performing a lamp test using the ACO/LAMP TEST button

Use this procedure to test for defective lamps by pressing the ACO/LAMP TEST button.

> ***Note:*** The primary function of the ACO/LAMP TEST button is to silence alarms. If an audible alarm is present while the button is being pressed, the alarm will be silenced. The button will have to be pressed again to perform a lamp test.

When a lamp test is performed on an access bandwidth manager (ABM) shelf, using the ACO/LAMP TEST button on the LCAP, all lamps on the BIP and on the shelf circuit packs are tested for 30 seconds.

When a lamp test is performed on the transport bandwidth manager (TBM) shelf, using the ACO/LAMP TEST button on the LCAP, only the circuit pack LEDs are tested for 30 seconds, and not the lamps on the TBM BIP. To test the lamps on the TBM BIP, the ACO/LAMP TEST button must be pressed on the BIP. The TBM BIP lamps light as long as the button is depressed.

> ***Note:*** The "Active" LED on the standby processor will not light if a restart is in progress, or if communication to the standby processor is down. The "Active" LED on the standby processor may turn off before other LEDs, if the active processor undergoes a restart, or may turn off after other LEDs, if the standby processor undergoes a restart during the lamp test.

Requirements

None

—continued—

Procedure 8-4 (continued)
Performing a lamp test using the ACO/LAMP TEST button

Action

Step	Action

If testing	Then
lamps on a TBM BIP	start at step 1
LEDs on a TBM shelf circuit packs	start at step 2
LEDs on ABM shelf circuit packs, and lamps on the ABM BIP	start at step 3

1 To test the TBM BIP lamps, press the ACO/LAMP TEST button on the TBM BIP.

The functional BIP lamps light while the button is pressed.

If a BIP lamp does not light during the test, replace the lamp. See *Routine Maintenance Procedures*, 323-3001-546, in *Maintenance*, Volume 5C.

2 To test the LEDs on circuit packs mounted in the TBM shelf, press the ACO/LAMP TEST button on the local craft access panel (LCAP) twice.

The functional circuit pack LEDs light for 30 seconds.

If a circuit pack LED does not light during the test, replace the circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If you do not have additional ABM lamp tests to perform, end the procedure. If you do have ABM lamp tests to perform, continue to the next step.

3 To test the LEDs on circuit packs mounted in the ABM shelf, and to test lamps on the ABM BIP, press the ACO/LAMP TEST button on the local craft access panel (LCAP) twice.

The functional circuit pack LEDs and BIP lamps light for 30 seconds.

If a BIP lamp does not light during the test, replace the lamp. See *Routine Maintenance Procedures*, 323-3001-546, in *Maintenance*, Volume 5C. For BIPs with an LED card, see *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

If a circuit pack LED does not light during the test, replace the circuit pack. See *Module Replacement Procedures*, 323-3001-547, in *Maintenance*, Volume 5C.

4 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Procedure 8-5
Performing a manual diagnostic test

Use this procedure to manually run a diagnostic test on any of the following circuit packs:

- processor (PROC)
- transport interface card (TIC)
- access interface card (AIC)
- maintenance interface card (MIC)
- test access card (TAC)
- integrated remote test unit (IRTU)
- narrowband line interface card (LIC)
- metallic test access card (MTAC)
- line card (LC)
- OC12: VTBM or SRP

Diagnostics can be run on an in-service or out-of-service PROC, TIC, AIC, MIC, IRTU, LIC, MTAC or OC12.

Diagnostics can only be run on an out-of-service TAC or line card.

Out-of-service diagnostics are more extensive than in-service diagnostics. Diagnostic failures appear in log report EQP322; log EQP609 reports passes.

Requirements

- Read the commands conventions described in *Network Element User Interface Description*, 323-3001-300, in *Operations, Administration, and Provisioning*, Volume 4A.
- When performing a manual diagnostic test on an access interface card (AIC) or a narrowband line interface card (NLIC), the operating state must not be Parent Eqpt Unavail (PEU). If the operating state is PEU, the manual diagnostic cannot be run.
- The user must be logged in with admin privileges to perform this procedure.

—continued—

Procedure 8-5 (continued)
Performing a manual diagnostic test

Action

Step	Action

1 From the Network Element Status screen, display the required equipment screen:

If diagnosing	Then do
TIC, AIC, Proc, MIC, TAC, IRTU or OC12	a.
LIC or MTAC	b.
LC	c.

a. Display the required equipment screen:

eq <type> <group>↵
where

< type >	circuit pack: **aic, proc, tic, mic, tac** or **OC12**
< group >	number of the group: For a TIC, AIC, or Proc: **a** or **b** For MIC, TAC or IRTU: no group required For OC12: g1 or g2

If performing diagnostics on a card that is	Then go to
out-of-service (OOS)	step 3
in-service (IS)	step 2

b. Display the detailed equipment screen:

eq <type>;<details> <CDS #> <group>↵
where

<type>	type of circuit pack: **lic** or **mtac**
<details>	LIC or MTAC details screen: **dtllic** or **dtlmtac**
<CDS #>	copper-distribution shelf housing the LIC: **1** to **7**
< group>	group number of the LIC: **a, b, c,** or **d**

If performing diagnostics on a card that is	Then go to
out-of-service (OOS)	step 3
in-service (IS)	step 2

—continued—

Procedure 8-5 (continued)
Performing a manual diagnostic test

Step	Action

c. Display the line card equipment screen:

eq lc <CDS #> <LC #>↵

where

<CDS #>	copper-distribution shelf number: **1** to **7**
<LC #>	line card number: **1** to **96**

If performing diagnostics on a card that is	Then go to
out-of-service (OOS)	step 3
in-service (IS)	step 2

2 Change the state to out-of-service:

chgstate oos↵
y↵

When changing the state of a card to OOS the card must first be put into standby mode.

Note: Diagnostics can only be run on an out-of-service TAC or line card.

3 Start the manual diagnostic test:

diagnose↵

The system displays the following response:

```
The diagnostics may take some time.
Do you want to continue?
Please confirm (yes or no)
```

4 Confirm or cancel the request:

To continue with the test:

yes↵

To cancel the test:

no↵

Diagnostic failures are reported in log EQP322; passes are reported in log EQP609.

—continued—

Procedure 8-5 (continued)
Performing a manual diagnostic test

Step	Action
5	To view the log report: **admin nep;logs;open eqp**↵ ***Note:*** The command **logutil** can also be used to access the Log Report utility.

If log	Then
EQP322 is reported	See *Log Report Manual*, 323-3001-840, in *Maintenance*, Volume 5B, for the appropriate action to take.
EQP609 is reported	The manual diagnostic test was completed successfully. End the procedure.

6	If you cannot successfully complete this procedure, contact your next level of support.

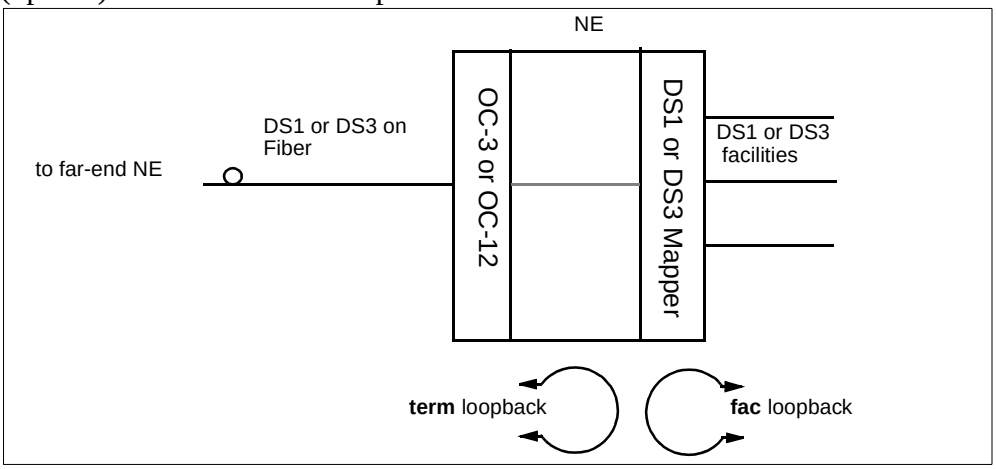
—end—

Procedure 8-6
Setting or releasing a loopback on a DS1 or DS3 facility

CAUTION
Risk of service loss
If you are testing DS1s using loopbacks and your system is provisioned for superframe frame format, AMI line coding, and bytesynchronous synchronization mode, do not use the 3 in 24 or 1 in 8 test patterns. If you do use these patterns, traffic will not be restored if you remove the loopback and re-insert it. (To restore traffic, place the facility out of service and then back in service.)

Use this procedure to set or release a loopback on a DS1 or DS3 facility. Two types of loopback can be set: facility (fac) and terminal (term).

A facility loopback takes the incoming (copper) DS1 or DS3 and loops it back to the source, as shown following. A terminal loopback takes the incoming (optical) DS1 or DS3 and loops it back to the far-end network element.



—continued—

Procedure 8-6 (continued)
Setting or releasing a loopback on a DS1 or DS3 facility

Action

Step	Action
1	From the Network Element Status screen, display the DS1 or DS3 facility screen: **fa < type > < group > < port >**↵ where < type > — type of DS facility: **ds1** or **ds3** < group > — number of the circuit pack group: See “Group and slot associations for DS1 and DS3” on page 24. < port # > — number of the port: For DS1**: 1** to **14** For DS3: **1, 2,** or **3** *The DS1 or DS3 facility screen appears.*
2	Take the facility out of service: **chgstate oos** ↵ **y**↵ *The operating state changes to out-of-service (OOS).*

—continued—

Procedure 8-6 (continued)
Setting or releasing a loopback on a DS1 or DS3 facility

Step	Action

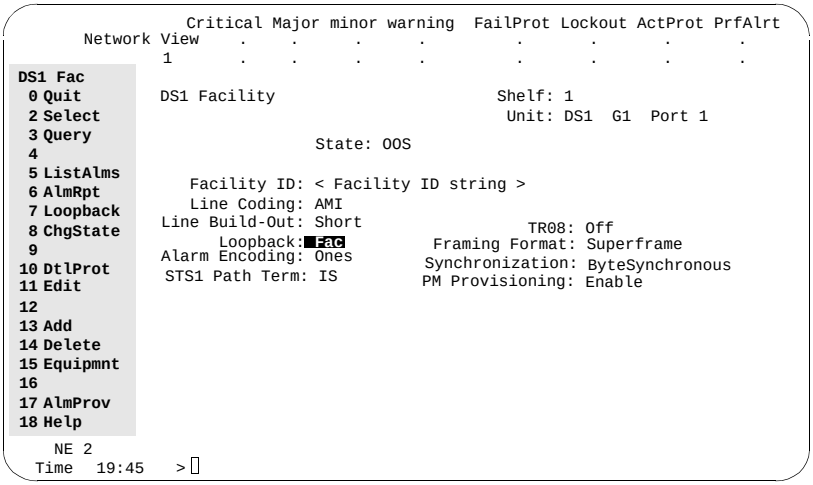
3 Operate or release the loopback:

loopback < action > < type >↵

where

< action >	operates or releases the loopback: **op** or **re**
< type >	for the *op* action, specifies the type of loopback: **fac** or **term** (see page 8-14 for an explanation) No need to specify type when releasing loopback.

The following DS1 facility screen shows the status of the loopback in reverse video.



4 If you released the loopback in step 3, return the facility to in-service (IS):

chgstate is↵

The operating state changes to in-service (IS).

5 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Procedure 8-7
Manually switching processor activity from active to standby

Use this procedure to switch processor activity from the currently active processor to the standby processor. There must be a backup processor in the in-service state, with valid data and an initialized software load.

The force option in the following procedure should be used only when both processors are faulty, and you want to switch activity to the processor with the less severe fault. This procedure affects GR-303 calls in progress for a period of about 30 seconds.

> ***Note:*** If you use the *force* option to switch activity from a trouble-free processor to a faulty processor, the system will automatically switch activity back to the trouble-free processor.

Requirements

Read the command conventions in *Network Element User Interface Description*, 323-3001-300, in *Operations, Administration, and Provisioning*, Volume 4A.

Action

Step	Action
1	From the Network Element Status screen, display the processor equipment screen: **eq proc <group>**↵ where <group> processor group number: **a** or **b**

—continued—

Procedure 8-7 (continued)
Manually switching processor activity from active to standby

Step	Action

CAUTION
Possible loss of service
DS1 and DS3 protection switching is unavailable during a switch of activity (SWACT) of the processor cards. If a DS1/VT mapper or a DS3/STS mapper fails while a SWACT is in progress, traffic cannot be switched to the protection mapper. Protection switching is available (after the SWACT) when the user is prompted to log in to the network element.

2 Switch activity to the backup (redundant unit) processor.

Note: Only use the *force* option in the following command string when both processors are faulty, and you want to force activity to the processor with the less severe fault.

switch [force]↵

The system prompts for confirmation of the switch request.

Note: During a processor card SWACT, the green active LED on working DS1/VT mappers and DS3/STS mappers goes out for approximately 20 seconds. The DS1/DS3 mappers are fully functional during this 20 second interval and there is no loss of traffic.

3 Confirm or cancel the switch request:

To confirm the switch:

y↵

To cancel the switch:

n↵

Processor activity switches to the backup processor within 5 seconds and the Active LED on the card is updated. After logging back in to the NE, the Protection State field on the screen changes from standby to active.

If you switch activity from a trouble-free processor to a faulty processor, the system automatically switches activity back to the trouble-free processor.

4 You must log back in to the network element user interface.

Note: You must wait 7 minutes before performing another protection switch on the same processor cards.

5 If you cannot successfully complete this procedure, contact your next level of support.

—end—

Procedure 8-8
Manually restarting the processor

CAUTION
Loss of service
Call NT support before performing a restart on the active processor card. A reload restart or a cold restart on the active processor causes all locally switched calls to be dropped.

Use this procedure to perform a warm, cold or reload restart on the active processor card or a reload restart on the inactive processor card.

During a restart of the active processor, DS1 protection is unavailable, and service may be affected. The restart does not cause a switch of activity from one processor to the other.

Reload restart on the active processor card

A reload restart is the most severe form of restart. The system effects of a reload restart are as follows:

- the shelf is re-provisioned
- all locally switched calls are dropped
- non-locally switched calls are maintained
- non-switched calls are maintained
- all equipment is restored to the provisioned state
- the current session on the user interface is dropped and the user is logged off
- the current performance monitoring information is lost (including logs)
- the system re-evaluates active alarms
- all data link ports for EOC, CSC, EMC, TBL, and SOH DCC are initialized

Cold restart on the active processor card

A cold restart is more severe than a warm restart but less severe than a reload restart. The effects of a cold restart are as follows:

- all locally switched calls are dropped
- non-locally switched calls are maintained
- non-switched calls are maintained

—continued—

- equipment is maintained in its current state; however, all transient maintenance actions are dropped
- the system is not re-provisioned
- the current session on the user interface is dropped and the user is logged off
- current performance monitoring information is maintained
- all active alarms are maintained
- all data link ports for EOC, CSC, EMC, TBL, and SOH DCC are initialized

Warm restart on the active processor card

A warm restart is the least severe restart type. The effects of a warm restart are as follows:

- stable locally switched calls in the talking state are maintained
- non-locally switched calls are maintained
- non-switched calls are maintained
- equipment is maintained in its current state; however, all transient maintenance actions are dropped
- the system is not re-provisioned
- the current session on the user interface is dropped and the user is re-logged in by the system after the restart is completed
- current performance monitoring information is maintained
- all active alarms are maintained
- all data link ports for EOC, CSC, EMC, TBL, and SOH DCC are initialized

Reload restart on the inactive processor card

A reload restart on the inactive processor card causes the inactive processor card to be reloaded.

Requirements

Read the commands conventions described in *Network Element User Interface Description*, 323-3001-300, in *Operations, Administration, and Provisioning*, Volume 4A.

You must log in to the network element.

The restart cannot be performed if either of the following alarms is raised: “Loss of mate communication” or “Circuit pack missing”.

—continued—

Procedure 8-8 (continued)
Manually restarting the processor

Action

Step	Action

If entering command at	Then
CI level	go to step 1
Proc equipment screen	go to step 3

1 From the CI level, perform the restart on the active processor:

restart <type>↵

where

<type>	type of restart to be performed: **warm, cold,** or **reload**

The system prompts for confirmation.

2 Confirm the restart:

y↵

The processor restarts. The restart time depends on the type of restart.

End the procedure here.

3 From the Network Element Status screen, display the processor screen for the working processor:

eq proc <group>↵

where

< group>	group number of the working processor: **a** or **b**

The processor equipment screen appears.

—continued—

Procedure 8-8 (continued)
Manually restarting the processor

Step	Action
4	Restart the processor: **restart <type>**↵ where <type> type of restart to be performed: **warm, cold,** or **reload** *The system prompts for confirmation of the restart.*
5	Confirm or cancel the restart: To confirm the restart, enter: **yes**↵ To cancel the restart, enter: **no**↵ *On the active processor, the restart is delayed by 5 seconds to allow the UI response to be displayed. On the standby processor, the restart begins immediately. The restart time depends on the type of restart.* When the network element user interface session closes during a restart of the active processor, the following text appears on the screen if you are accessing the NE from the OPC: `Press Return to exit.`
6	Log in to the network element again.
7	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Procedure 8-9
Manually restarting the shelf

CAUTION
Loss of service
Call NT support before performing a shelf restart. A reload restart or a cold restart causes all locally switched calls to be dropped.

Use this procedure to restart the processor software for a network element common-equipment shelf.

Shelf Restart Types

The three types of shelf restarts are reload restart, cold restart and warm restart.

Reload restart

A reload restart is the most severe form of restart. The system effects of a reload restart are as follows:

- the shelf is re-provisioned
- all locally switched calls are dropped
- non-locally switched calls are maintained
- non-switched calls are maintained
- all equipment is restored to the provisioned state
- the current session on the user interface is dropped and the user is logged off
- the current performance monitoring information is lost (including logs)
- the system re-evaluates active alarms
- all data link ports for EOC, CSC, EMC, TBL, and SOH DCC are initialized

Cold restart

A cold restart is more severe than a warm restart but less severe than a reload restart. The effects of a cold restart are as follows:

- all locally switched calls are dropped
- non-locally switched calls are maintained
- non-switched calls are maintained

—continued—

- equipment is maintained in its current state, however, all transient maintenance actions are dropped
- the system is not re-provisioned
- the current session on the user interface is dropped and the user is logged off
- current performance monitoring information is maintained
- all active alarms are maintained
- all data link ports for EOC, CSC, EMC, TBL, and SOH DCC are initialized

Warm restart

A warm restart is the least severe restart type. The effects of a warm restart are as follows:

- stable locally switched calls in the talking state are maintained
- non-locally switched calls are maintained
- non-switched calls are maintained
- equipment is maintained in its current state, however, all transient maintenance actions are dropped
- the system is not re-provisioned
- the current session on the user interface is dropped and the user is re-logged in by the system after the restart is completed
- current performance monitoring information is maintained
- all active alarms are maintained
- all data link ports for EOC, CSC, EMC, TBL, and SOH DCC are initialized

Requirements

Read the commands conventions described in *Network Element User Interface Description,* 323-3001-300, in *Operations, Administration, and Provisioning*, Volume 4A.

You must log in to the network element.

The restart cannot be performed if either of the following alarms is raised: “Loss of mate communication” or “Circuit pack missing”.

—continued—

Procedure 8-9 (continued)
Manually restarting the shelf

Action

Step	Action
1	From the network element status screen, display the shelf equipment screen: **eq sh**↵ *The Shelf Equipment screen appears.*
2	Perform a shelf restart by entering: **restart < type >**↵ where < type > type of restart to be performed: **warm, cold,** or **reload** *The system prompts for confirmation of the restart.*
3	Confirm or cancel the restart: To confirm the restart enter: **yes**↵ To cancel the restart enter: **no**↵
4	The restart is delayed by 5 seconds to allow the UI response to be displayed. The restart time depends on the type of restart. When the network element user interface session closes, the following text appears on screen if you are accessing the NE from the OPC: *Press Return to exit.*
5	Log in to the network element again.
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Procedure 8-10
Resetting a line card

Use this procedure to reset a line card in the copper-distribution shelf. The reset causes the line card to be reloaded, if appropriate, and performs a long diagnostic on the line card.

A line card reset can be performed on an in-service or out-of-service line card. Diagnostic passes appear in log report LC602 and failures in log LC307.

Requirements

Read the commands conventions described in *Network Element User Interface Description*, 323-3001-300, in *Operations, Administration, and Provisioning*, Volume 4A.

Action

Step	Action

1 Display the line card equipment screen:

eq lc <CDS #> <LC #>↵

where

<CDS #>	copper-distribution shelf number: **1** to **7**
<LC #>	line card slot number: **1** to **96** ***Note:*** For Omega 4-wire and Omega 6- 8-wire line cards, use the lowest even slot number occupied by the card.

The line card equipment screen appears.

2 Reset the line card:

resetlc ↵

The system prompts for confirmation with the following message:

```
ResetLC
Note: RESETLC command will reboot the software.
Do you wish to proceed?
Please confirm ("Yes" or "No"):
```

—continued—

Procedure 8-10 (continued)
Resetting a line card

Step	Action
3	Confirm the reset: **yes** ↵ *The system confirms the reset with the following message:* `The ResetLC command has been received.It will be processed. Please refer to LC logs for results.` ***Note:*** Once the reset command is confirmed, the line card is reloaded by the system, if appropriate, then a long diagnostic is performed. Diagnostic failures are reported in log LC307. Diagnostic passes are reported in log LC602.
4	To view the log report: **admin nep;logs;open <type>** ↵ where <type> — The type of log report**:** For equipment other than line cards: **eqp** For line cards: **lc**
5	If you cannot successfully complete this procedure, contact your next level of support. **—end—**

Procedure 8-11
Diagnosing failed CDS circuit packs

Use this procedure to diagnose common-equipment circuit packs in a copper-distribution shelf (LIC, MTAC, or CDSP), or to verify failure of circuit packs with a red LED illuminated.

Requirements

Read the commands conventions described in *Network Element User Interface Description*, 323-3001-300, in *Operations, Administration, and Provisioning*, Volume 4A.

Action

Step	Action
1	Log in to the network element user interface.
2	If you wish to diagnose an MTAC circuit pack, skip to step 7. If you wish to diagnose a LIC or CDSP circuit pack, continue at step 3.
3	If a LIC or CDSP circuit pack in a copper-distribution shelf indicates trouble or failure by its red LED being lit, you can perform out-of-service (OOS) diagnostics on the failed circuit pack. Display the detailed equipment screen for the appropriate circuit pack as follows: If the circuit pack is a line interface card, enter: **eq lic** ↵ **dtllic < CDS # > < ID >** ↵ If the circuit pack is a CDS power card, enter: **eq cdsp** ↵ **dtlcdsp < CDS # > < ID >** ↵ where CDS # — copper-distribution shelf number; enter one of **1** to **7** ID — equipment instance; enter one of **a**, **b**, **c**, or **d** for LICs, or **a** or **b** for CDSPs

—continued—

Procedure 8-11 (continued)
Diagnosing failed CDS circuit packs

Step	Action
4	If the module to be diagnosed is not already out of service, enter: **chgstate oos** ↵ *Confirmation is requested. If you confirm the action, the State field value changes to OOS.*
5	Initiate diagnostics, by entering: **chgstate is** ↵ ***Note:*** The **diagnose** command can also be used to initiate diagnostics. *The system performs out-of-service diagnostics on the module as part of the transition from an OOS state to an in-service (IS) state.* *Diagnosis can take a while; it proceeds as a background task. The diagnosis is reported as an update to the state of the circuit pack, as follows:* OOS-MTCE DIAGNOSE — diagnostics in progress OOS-TSTF — diagnostics failed IS-NR — diagnostics passed
6	If failure is indicated, remove the defective module and insert a spare module.
7	If the circuit pack is a metallic test access card, enter: **eq mtac** ↵ **dtlmtac < CDS # > < ID >** ↵ where CDS # — copper-distribution shelf number; enter one of **1** to **7** ID — equipment instance; enter one of **a** or **b** for MTACs
8	If the MTAC to be diagnosed is not already out of service, enter: **chgstate oos** ↵ *Confirmation is requested. If you confirm the action, the State field value changes to OOS.* ***Note:*** On an MTAC, out-of-service diagnostics are not automatically conducted during the transition from an OOS state to an IS state. It is necessary to use the “diagnose” command to invoke diagnostics.

—continued—

Procedure 8-11 (continued)
Diagnosing failed CDS circuit packs

Step	Action
9	Initiate diagnostics, by entering: **diagnose** ↵ *The system performs out-of-service diagnostics on the MTAC.* ***Note:*** When diagnostics are requested on an MTAC and the resources are busy, the diagnostic request is rejected. If diagnostics are requested on an MTAC which is not out-of-service, the diagnostic request is rejected. *Diagnosis can take a while; it proceeds as a background task. The diagnosis is reported as an update to the state of the circuit pack, as follows:* OOS-MTCE DIAGNOSE — diagnostics in progress OOS-TSTF — diagnostics failed OOS — diagnostics passed
10	If failure is indicated, remove the defective MTAC and insert a spare one. Check that the MTAC goes in service. *The new MTAC undergoes self-tests. If it passes, it goes in service.* **If the MTAC** / **Then** goes in service — Go to step 13. stays out of service — Go to step 11.
11	If the new MTAC fails or more than one MTAC fails diagnostics, there may be a higher order problem, such as loose cables, bent pins, TAC fault, or other condition. Check for raised alarms, especially TAC alarms. **If there are** / **Then** raised alarms — Look up the alarm in this book and follow the appropriate alarm clearing procedure to clear the alarm. no raised alarms — Go to step 12.
12	Check for hardware problems on the CDS, such as bent pins and loose cables. **If there are** / **Then** hardware problems — Fix the hardware problem. If you cannot fix the hardware problem, contact your next level of support. no hardware problems — Contact your next level of support.

—continued—

Procedure 8-11 (continued)
Diagnosing failed CDS circuit packs

Step	Action
13	If the MTAC passed diagnostics, place it back in service, by entering: **chgstate is** ↵ *The MTAC goes in service.*
14	Repeat the applicable steps of this procedure for any other circuit packs which you wish to diagnose.
15	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Procedure 8-12
Generating alarms for testing purposes

Use this procedure to generate critical, major, minor, or warning alarms, in order to test the operation of the alarm system.

Requirements

Read the commands conventions described in *Network Element User Interface Description*, 323-3001-300, in *Operations, Administration, and Provisioning*, Volume 4A.

Action

Step	Action
1	Access the FiberWorld Alarm Test CI (fwaltsci) tool from the command interpreter (CI) level of the user interface, or from any FWPUI screen: **fwaltsci** ↵ *The following prompt appears: "fwaltsci".*

If you want to	Then
display the current state of the test alarms	go to step 2
generate a test alarm	go to step 3
clear a test alarm	go to step 4

2 Display the current state of the test alarms:

display ↵

A list appears showing the state of each alarm severity. A list is shown in the following example:

```
Status of test alarms:
Warning:   Clear
Minor:     Clear
Major:     Raised
Critical:  Clear
```

—continued—

Procedure 8-12 (continued)
Generating alarms for testing purposes

Step	Action
3	Generate a test alarm: **raise <severity>** ↵ where < severity > is the severity of the test alarm to be raised: **warning, minor, major,** or **critical** *A test alarm of the specified severity is raised. This alarm will appear in the list of alarms on the user interface, and will activate the appropriate alarm relay contacts.*
4	Clear a test alarm: **clear <severity>** ↵ where < severity > is the severity of the test alarm to be cleared: **warning, minor, major,** or **critical** *The test alarm of the specified severity is cleared.*
5	Quit from the fwaltsci tool: **quit**↵
6	If you cannot successfully complete this procedure, contact your next level of support.

—end—

Index

A

ABM shelf
  functions
    DS1 circuit pack groups 1-17
    DS3 circuit pack groups 1-18
Access failure
  clear alarm 3-42
Access interface card
  equipment troubleshooting 3-20
  LED, troubleshooting 7-12
Access Interface Card. See AIC
ACO
  command
    silencing alarms 1-5
  failure
    causes 1-5
ACO/LT button
  local craft access panel 1-5
AIC
  alarm 1-10
  failure
    troubleshooting 3-63, 3-65
Alarm 2-6, 3-335
  access interface card 1-10
  ACO failure 1-5
  audible, silencing 1-5
  circuit packs 2-5
  class 1-9
    Env (Environmental) 5-1
    Eqp (Equipment) 3-1
    Fac (Facility) 4-1
  clearing 1-8
    how to begin 1-2
    how to look up alarm procedures 1-12
  COMM facility
    faulty path 4-10
Alarm (continued)
  common-equipment 1-10
  common-equipment circuit pack
    OPC, MIC, and ESI 2-7
  copper-distribution shelf 1-10
  copper-distribution shelf power 1-10
  critical
    both planes non-operational 3-48
    circuit pack fail 3-20, 3-80, 3-115
    circuit pack mismatch 3-21, 3-81, 3-116
    circuit pack missing 3-22, 3-83, 3-117
    comm overhead clock/frame loss 3-23
    comm overhead data loss 3-24
    critical test alarm 3-53
    D-link interface fail 3-26
    input card mismatch 3-87
    input card missing 3-88
    line RFI 4-126
    output card mismatch 3-92
    output card missing 3-93
    prot bridge in card mismatch 3-95
    prot bridge in card missing 3-96
    prot bridge out card mismatch 3-98
    prot bridge out card missing 3-99
    protection version mismatch 3-110
    required action 1-8
    service effects 1-8
    shelf assembly fail 3-68
    STS1 intercard fail 3-111, 3-129
    switcher circuit pack mismatch 3-131
    switcher circuit pack missing 3-132
    T-link interface fail 3-30, 3-31, 3-198
  degradation of service 1-8
  digital test access pair 1-10
  display priority 1-4
  DS1 transport 1-10

Alarm (continued)
DS3 transport 1-10
environmental
48 V dc CDS breaker tripped ext bay 5-21
48 V dc CDS breaker tripped main bay 5-22
48V battery A CE supply fail 5-15
48V battery B CE supply fail 5-18
high CE shelf temperature 5-10
equipment 3-1, 3-20, 3-22, 3-43, 3-80, 3-115, 3-333
access failure 3-42
autoprovisioning mismatch 3-47
BNC I/O card 1 fail 3-330
BNC I/O card 1 fail -DoNotRemove 3-112
BNC I/O card 1 mismatch 3-113, 3-331
BNC I/O card 1 missing 3-114, 3-332
BNC I/O card 2 fail -DoNotRemove 3-112
BNC I/O card 2 mismatch 3-113
BNC I/O card 2 missing 3-114
BNC I/O card 3 fail -DoNotRemove 3-112
BNC I/O card 3 mismatch 3-113
BNC I/O card 3 missing 3-114
both planes non-operational 3-48
circuit pack mismatch 3-21, 3-44, 3-81, 3-116, 3-334
circuit pack missing 3-45, 3-83, 3-117
clock failure 3-46
comm overhead data loss 3-24
critical test alarm 3-53
data available 2-5
database not restored. Type Q APPROVE at NE 3-54
datasync fail 3-293
default K bytes 3-260
D-link interface fail 3-26
DS1 or DS3 2-6
end VCO range 3-141
entry to SONET clock acquire 3-264
entry to SONET clock freerun 3-56
entry to SONET clock holdover 3-266
equipment forced switch request 3-142
equipment lockout request 3-143
Alarm, equipment (continued)
equipment manual switch request 3-144
equipment protection switch complete 3-145
equipment protection switch fail 3-146
exerciser fail 3-59
facility provisioning mismatch 3-84, 4-184, 4-203
failure to lock 3-147
firmware failure 3-336
firmware version mismatch 3-29, 3-206
firmware/software incompatible 3-337
forced switch request 3-85, 3-338
input card fail -DoNotRemove 3-86
input card mismatch 3-87
input card missing 3-88
intercard fail 3-148
invalid neighbor detected 3-273
LED driver fail 3-209
lockout protection operation fail 3-241
lockout protection request 3-275
lockout request 3-89, 3-119, 3-242, 3-339
lockout working request 3-276
loss of data synchronization 3-60
lost peer OPC 3-294
major test alarm 3-60, 3-61
manual switch request 3-90, 3-120, 3-340
minor test alarm 3-62
output card fail -DoNotRemove 3-91
output card mismatch 3-92
output card missing 3-93
plane A non-operational 3-63
plane B non-operational 3-65
plane messaging corruption 3-30, 3-198
power filter A missing 3-36
power filter B missing 3-39
prot bridge in card failed 3-94
prot bridge in card mismatch 3-95
prot bridge in card missing 3-96
prot bridge out card failed 3-97
prot bridge out card mismatch 3-98
prot bridge out card missing 3-99
protection path fail 3-101, 3-121, 3-341
protection switch complete 3-105, 3-124, 3-344

Alarm, equipment (continued)
protection switch fail 3-106, 3-126, 3-345
protection version mismatch 3-110
shelf assembly fail 3-68
shelf ID bus fail 3-69
software trap 3-70
SONET overhead clock loss 3-71
STS-1 intercard fail 3-111, 3-129, 3-347
subunit mismatch 3-150
subunit, fail 3-149
subunit, missing 3-151
switcher circuit pack mismatch 3-131, 3-348
switcher circuit pack missing 3-132, 3-349
tape backup/restore fail 3-309
Threshold 1 DS0 exceeded 3-34
Threshold 2 DS0 exceeded 3-34
timing generation primary reference fail 3-73
timing generation secondary reference fail 3-73
timing generation, entry to acquire 3-152
timing ref lockout request 3-405
timing ref prot oscillation control activated 3-406
timing ref prot switch complete 3-407
timing ref prot switch fail 3-408
T-link interface fail 3-30, 3-31, 3-198
traffic problem detected 3-133, 3-350
traffic upgrade in progress 3-77
VT connection provisioning mismatch 3-136
warning test alarm 3-78, 3-80
external equipment 2-2
external synchronization interface 1-10
facility 4-1
frequency out of range 4-68
high traffic threshold exceeded 4-23
laser bias current 4-125
line FE CV threshold 4-70
line FE ES threshold 4-70
line FE SES threshold 4-70
line RFI 4-126
line Rx CV threshold 1, 2 4-24
Alarm, facility (continued)
line Rx ES threshold 1, 2 4-24
line Rx SES threshold 1, 2 4-24
loopback 4-27, 4-167
loss of frame 2-2
low traffic threshold exceeded 4-28
path Rx CV threshold 1, 2 4-29
path Rx ES threshold 1, 2 4-29
path Rx SAS threshold 1, 2 4-29
path Rx SES threshold 1, 2 4-29
path Rx UAS threshold 1, 2 4-29
PRI link OOS 4-32, 4-183
Rx AIS 4-33
Rx bipolar violation 4-168
Rx bipolar violation>10E-3 4-35
Rx line AIS 4-178
Rx loss of frame 4-39, 4-171
Rx loss of pointer 4-174
Rx loss of signal 4-42, 4-175
Rx RFI 4-179
Rx yellow 4-44
STS-1 path CV threshold 1,2 4-45
STS-1 path ES threshold 1,2 4-45
STS-1 path FE CV threshold 1,2 4-89
STS-1 path SES threshold 1,2 4-45
STS-1 path UAS threshold 1,2 4-45
STS-1 Rx AIS 4-152
STS-1 RX loss of pointer 4-156
STS1 Rx path trace failure 4-50
STS-1 Rx RFI 4-53, 4-93, 4-187
STS1 Rx unequipped 4-55
STS-1 signal label mismatch 4-57, 4-96
STS1 signal label mismatch 4-57
VT Rx AIS 4-58
VT Rx loss of pointer 4-60
VT Rx RFI 4-64
VT Rx unequipped 4-66
facility COMM
faulty path 4-10
generating, for testing purposes 8-32
hierarchy 2-2
AccessNode circuit packs 2-8
circuit pack 2-5
circuit pack failures 2-2
common-equipment circuit pack 2-7
diagnostics 2-6
environmental 2-8

Alarm, hierarchy (continued)
equipment 2-5, 3-1
facility 2-2
inter-card failures 2-2
MIC Circuit pack fail 2-7
parent equipment 2-8
processor common-equipment 2-7
serial telemetry port failure 2-7
switcher circuit pack missing 2-5
telemetry latch 2-8
indication signal 2-2
integrated remote test unit 1-10
interpreting information 1-1, 1-7
line card 1-10
line interface card 1-11
loss of frame 2-2
maintenance interface card 1-11
major
BNC I/O card x fail -DoNotRemove 3-112
BNC I/O card x mismatch 3-113
BNC I/O card x missing 3-114
circuit pack fail 3-43
circuit pack mismatch 3-44
circuit pack missing 3-45
facility provisioning mismatch 3-84, 4-184, 4-203
failure to lock 3-147
input card fail -DoNotRemove 3-86
intercard fail 3-148
invalid neighbor detected 3-273
major test alarm 3-61
output card fail -DoNotRemove 3-91
prot bridge in card fail -DoNotRemove 3-94
prot bridge out card fail -DoNotRemove 3-97
protection path fail 3-101, 3-121
required action 1-8
service effects 1-8
shelf ID bus fail 3-69
STS-1 Rx RFI 4-53
subunit fail 3-149
subunit mismatch 3-150
subunit missing 3-151

Alarm, major (continued)
timing generation primary reference fail, when both primary and secondary are in alarm status 3-74
traffic problem detected 3-133
metallic test access card 1-11
MIC Circuit pack fail 2-7
minor
autoprovisioning mismatch 3-47
BNC I/O card x fail -DoNotRemove 3-112
circuit pack fail 3-20, 3-43, 3-80, 3-115
circuit pack mismatch 3-21, 3-44, 3-81, 3-116
circuit pack missing 3-22, 3-45, 3-83, 3-117
CNet link fail 3-51
comm overhead clock/frame loss 3-23
comm overhead data loss 3-24
database not restored. Type Q APPROVE at NE 3-54
datasync fail 3-293
D-link interface fail 3-26
equipment forced switch request 3-142, 3-264
equipment lockout request 3-143
equipment manual switch request 3-144
equipment protection switch fail 3-146
exerciser fail 3-59
failure to lock 3-147
forced switch request 3-85, 3-118
input card fail -DoNotRemove 3-86
input card mismatch 3-87
input card missing 3-88
intercard fail 3-148
lockout protection operation fail 3-241
lockout protection request 3-275
lockout request 3-89, 3-119
lockout working request 3-276
lost peer OPC 3-294
manual switch request 3-90, 3-120
minor test alarm 3-62
output card fail -DoNotRemove 3-91
output card mismatch 3-92
output card missing 3-93
power filter A missing 3-36
power filter B missing 3-39

Alarm, minor (continued)
prot bridge in card fail -DoNotRemove 3-94
prot bridge in card mismatch 3-95
prot bridge in card missing 3-96
prot bridge out card fail -DoNotRemove 3-97
prot bridge out card mismatch 3-98
prot bridge out card missing 3-99
protection path fail 3-101, 3-121
protection switch fail 3-106, 3-126
protection version mismatch 3-110
required action 1-8
service effects 1-8
software trap 3-70
SONET overhead clock loss 3-71
STS1 intercard fail 3-111, 3-129
subunit fail 3-149
subunit mismatch 3-150
subunit missing 3-151
switcher circuit pack mismatch 3-131
switcher circuit pack missing 3-132
tape backup/restore fail 3-309
timing generation primary reference fail 3-74
timing generation secondary reference fail 3-74
timing generation secondary reference fail, when both primary and secondary are in alarm status 3-74
T-link interface fail 3-30, 3-31, 3-198
traffic problem detected 3-133
VT connection provisioning mismatch 3-136
network element list 1-4
not service-affecting required action 1-8
not service-affecting service effects 1-8
obtaining list network element alarms 1-2
obtaining list operations controller interface alarms 1-2
OC-12 transport 1-11
OC-3 transport 1-11
operations controller 1-11
optical interface component failure 2-6

Alarm (continued)
optical-laser failure 2-6
processor circuit pack 1-11
report ID number 1-4
reporting and surveillance 1-1, 2-1
screening 2-2
service-affecting 1-7
required action 1-8
service effects 1-8
severity 1-7
critical 1-7, 1-8
major 1-7, 1-8
minor 1-7, 1-8
not service-affecting 1-8
service-affecting 1-8
warning 1-7, 1-8
silencing how to 1-5
removing alarm relay card 1-5
using ACO command 1-5
using ACO/LT button 1-5
using remote ACO 1-5
STS-1 transport 1-10
telemetry latch 2-8
test access card 1-11
testing critical 3-53
testing major 3-61
testing minor 3-62
testing warning 3-78
transport interface card 1-11
troubleshooting AIC equipment 3-20 to 3-32
troubleshooting CDSP equipment 3-42 to 3-46
troubleshooting CE equipment 3-47 to 3-78
troubleshooting COMM facility 4-10, 4-21
troubleshooting copper-distribution-shelf equipment 3-36 to 3-46
troubleshooting DS1 equipment 3-80 to 3-111
troubleshooting DS1 facility 4-24, 4-64
troubleshooting DS1 facility STS-1 4-50
troubleshooting DS1 facility VT1.5 4-58
troubleshooting DS3 equipment 3-112 to 3-136
troubleshooting DS3 facility 4-68, 4-99
troubleshooting DS3 facility STS-1 4-90
troubleshooting environmental 5-1
troubleshooting ESI equipment 3-141 to 3-157

Alarm, troubleshooting (continued)
ESI facility 4-101, 4-115
IRTU equipment 3-137, 3-158, 3-167
LC equipment 3-170, 3-181
LED 7-1 to 7-34
LIC equipment 3-182
metallic test access 6-1
MIC equipment 3-201, 3-218
MTAC equipment 3-220, 3-222
OC-12 equipment 3-226, 3-258
OC-12 facility 4-144, 4-145, 4-162
OC-12 NE equipment 3-288
OC-3 equipment 3-226, 3-258
OC-3 facility 4-144, 4-145, 4-162
OC-3/OC-12 facility 4-152, 4-156
OPC equipment 3-298
pair gain test controller/metallic test access 6-1
proc equipment 3-312, 3-325
STS-1 equipment 3-330 to 3-352
STS-1 facility 4-163 to 4-179
TAC equipment 3-354, 3-363
TIC equipment 3-366, 3-373
TIC facility 4-45, 4-89, 4-212
TIC facility VT1.5 4-204
TIC facility, STS1 4-45, 4-89
TXC equipment 3-374, 3-405
type 1-9
warning
access failure 3-42
clock failure 3-46
CNet performance degraded 3-52
D-link interface fail 3-26
end VCO range 3-141
entry to SONET clock freerun 3-56
equipment protection switch complete 3-145
not-service affecting
line FE CV threshold 4-70
not-service affecting, laser bias current 4-125
not-service affecting, line FE CV threshold 4-70
not-service affecting, line FE ES threshold 4-70
not-service affecting, line FE SES threshold 4-70
Alarm, warning (continued)
not-service affecting, line FE UAS threshold 4-70
plane A non-operational 3-63
plane B non-operational 3-65
protection switch complete 3-105, 3-124
required action 1-8
service effects 1-8
T-link interface fail 3-30, 3-31
traffic upgrade in progress 3-77
warning test alarm 3-78
Alarm clearing
48 V dc battery A
common equipment supply fail 5-15
48 V dc battery B
common equipment supply fail 5-18
48 V dc CDS breaker tripped
ext bay 5-21
main bay 5-22
Alarm Cut Off. See ACO
Alarm hierarchies 2-2
Alarm relay card
removing to silence alarm 1-5
Alarms
Facility COMM
list of 4-1
Facility DS1
list of 4-2
Facility DS3
list of 4-4
Facility ESI
list of 4-5, 4-6
Facility OC-12
list of 4-6
Facility OC-3/OC-12
list of 4-7
Facility STS1
list of 4-8
Facility TIC
list of 4-9
Alert 2-6
defined 1-8
Approve command
potential service affects 3-54
Autoprovisioning mismatch
clear alarm 3-47

B

B8ZS
AZC provisioning combination 3-110
B8ZS line coding and AZC alarm encoding
troubleshooting 3-84
BITS. See Building Integrated Timing Source
BNC I/O card 1 fail
clearing alarm 3-330
BNC I/O card 1 fail -DoNotRemove
clear alarm 3-112
BNC I/O card 1 mismatch
clear alarm 3-113
clearing alarm 3-331
BNC I/O card 1 missing
clear alarm 3-114
clearing alarm 3-332
BNC I/O card 2 fail -DoNotRemove
clear alarm 3-112
BNC I/O card 2 mismatch
clear alarm 3-113
BNC I/O card 2 missing
clear alarm 3-114
BNC I/O card 3 fail -DoNotRemove
clear alarm 3-112
BNC I/O card 3 mismatch
clear alarm 3-113
BNC I/O card 3 missing
clear alarm 3-114
BNC I/O card ID PROM failure
troubleshooting 3-112
Both planes non-operational
clear alarm 3-48
Breaker interface panel
model NT4K14
LEDs, troubleshooting 7-34
model NT7E56
LED, troubleshooting 7-34
testing the lamps 8-6, 8-8
Building integrated timing source
use as a reference timer 3-73

C

CBIC-based card failure
troubleshooting 3-68, 3-69
CDS. See Copper-Distribution shelf
CDSP. See Copper-distribution shelf power
CE. See Common-equipment
Circuit pack
alarm hierarchy 2-5
fail
clear alarm 3-20, 3-43, 3-80, 3-115, 3-333
failure
alarm 2-6
mismatch
alarm 2-6
missing
clear alarm 3-22, 3-45, 3-335
performing a manual diagnostic test 8-10
testing the LEDs 8-6, 8-8
Circuit pack mismatch
clear alarm 3-21, 3-44, 3-81, 3-116
clearing alarm 3-334
circuit pack missing
clear alarm 3-83, 3-117
Clock failure
clear alarm 3-46
CNet
cabling 3-52
connectors, unused
terminating 3-52
link fail
clear alarm 3-51
performance degraded
clear alarm 3-52
Comm overhead
clock/frame loss
clear alarm 3-23
data loss
clear alarm 3-24
Common-equipment
alarm 1-10
shelf
equipment troubleshooting 3-47
Common-equipment. See also Shelf 2-7
Communication (COMM)
facility troubleshooting 4-10
Control Network. See CNet
Copper-distribution drawer
troubleshooting LED 7-7
Copper-distribution shelf
alarm 1-10
equipment troubleshooting 3-36

Copper-distribution shelf power
alarm 1-10
Copper-distribution-shelf power converter
equipment troubleshooting 3-42
LED, troubleshooting 7-15
Critical alarm
both planes non-operational 3-48
circuit pack fail 3-20, 3-80, 3-115
circuit pack mismatch 3-21, 3-81, 3-116
circuit pack missing 3-22, 3-83, 3-117
comm overhead clock/frame loss 3-23
comm overhead data loss 3-24
critical test alarm 3-53
D-link interface fail 3-26
generation
using FWALTSCI tool 3-53
input card mismatch 3-87
input card missing 3-88
output card mismatch 3-92
output card missing 3-93
prot bridge in card mismatch 3-95
prot bridge in card missing 3-96
prot bridge out card mismatch 3-98
prot bridge out card missing 3-99
protection version mismatch 3-110
shelf assembly fail 3-68
STS1 intercard fail 3-111, 3-129
switcher circuit pack mismatch 3-131
switcher circuit pack missing 3-132
T-link interface fail 3-30, 3-31, 3-198
Critical default K bytes 3-260
Critical test alarm
clear alarm 3-53
Critical, not service-affecting alarm
critical test alarm 3-53
Critical, service-affecting alarm
both planes non-operational 3-48
circuit pack fail 3-80
circuit pack mismatch 3-81
circuit pack missing 3-83
input card mismatch 3-87
input card missing 3-88
output card mismatch 3-92
output card missing 3-93
prot bridge in card mismatch 3-95
prot bridge in card missing 3-96
prot bridge out card mismatch 3-98
Critical, service-affecting alarm (continued)
prot bridge out card missing 3-99
shelf assembly fail 3-68
switcher circuit pack mismatch 3-131
switcher circuit pack missing 3-132
Current filter mode
ESI 3-73

D

D/VT link access cable
reseating 3-27
Database not restored. Type Q APPROVE at NE
clear alarm 3-54
datasync fail
clear alarm 3-293
Default K bytes
clear alarm 3-260
Digital test access pair
alarm 1-10
D-link interface fail
clear alarm 3-26
DS1
alarm, equipment 2-6
equipment
troubleshooting alarms 3-111
facility
setting or releasing a loopback 8-14
troubleshooting 4-24
group and slot association 1-15
I/O card slots 1-16
input card ID PROM failure
troubleshooting 3-86
output card ID PROM failure
troubleshooting 3-91
protection bridge in card ID PROM failure
troubleshooting 3-94
protection bridge out card ID PROM failure
troubleshooting 3-97
protection hardware failure
troubleshooting 3-101
transport alarm 1-10
DS1/VT mapper
circuit pack failure
troubleshooting 3-80

DS1/VT mapper, LED (continued)
troubleshooting 7-27
product engineering codes 3-84
DS1/VT protection mapper mismatch
troubleshooting 3-81
DS3
alarm, equipment 2-6
facility
troubleshooting 4-68
group and slot association 1-15
I/O card slots 1-16
protection mapper
replacement 3-123
TBM FCOT_BLSR group limitations 1-15
transport
alarm 1-10
DS3/STS mapper
LED, troubleshooting 7-28
DTAP. See Digital Test Access Pair

E

End VCO range
clear alarm 3-141
Entry to SONET
clock acquire
clear alarm 3-264
clock freerun
clear alarm 3-56
clock holdover
clear alarm 3-266
Environmental alarm
hierarchy 2-8
troubleshooting 5-1
Epsilon station line card
LED, troubleshooting 7-16
EQP606 log generation 3-85, 3-89, 3-90, 3-105, 3-118, 3-119, 3-120, 3-124
EQP608 log
using to determine exerciser failure 3-59
Equipment
forced switch request
clear alarm 3-142
lockout request
clear alarm 3-143
manual switch request
clear alarm 3-144
Equipment (continued)
protection switch complete
clear alarm 3-145
protection switch fail
clear alarm 3-146
Equipment alarm
clearing 3-1
data available 2-5
DS1 or DS3 2-6
ESI
alarm
common-equipment circuit pack 2-7
card
LED, troubleshooting 7-31
ESI. See External synchronization interface
Event Browser tool
using to troubleshoot
communication problems 1-3
Exerciser fail
clear alarm 3-59
External synchronization interface
alarm 1-10
carrier
reseating 3-57
current filter mode 3-73
equipment troubleshooting 3-141
ESI freerun vs. SONET freerun 3-73
facility troubleshooting 4-101
status 3-73
temporary loss of synchronization 3-75
External synchronization interface. See ESI

F

Facility
alarm
loss of frame 2-2
alarm hierarchy 2-2
FE UAS threshold crossing
line FE UAS threshold 4-70
provisioning
mismatch alarm clearing 3-84, 4-184, 4-203
Facility alarms
list of 4-1
Facility COMM alarms
list of 4-1

Facility DS1 alarms
list of 4-2
Facility DS3 alarms
list of 4-4
Facility DSI alarms
list of 4-5, 4-6
Facility OC-12 alarms
list of 4-6
Facility OC-3
OC-12 alarms
list of 4-7
Facility STS1 alarms
list of 4-8
Facility TIC alarms
list of 4-9
Failure to lock
clear alarm 3-147
FE UAS threshold crossing
line FE UAS threshold 4-70
Fiber-optic cable
verifying connections 3-71
Firmware failure
clearing alarm 3-336
Firmware version mismatch
clear alarm 3-29
clearing alarm 3-206
Firmware/software incompatible
clearing alarm 3-337
Forced switch
causing critical alarm 3-95, 3-96
releasing 3-85
request
clearing alarm 3-85, 3-338
releasing 3-142
FWALTSCI tool
using to test critical alarm 3-53
using to test generation of minor alarm 3-62
using to test major alarm 3-61
using to test warning alarm 3-78

G

Group and slot association
DS1, DS3, STS-1, OC-3, OC-12 1-15

H

High CE shelf temperature
clearing alarm 5-10

I

I/O card
troubleshooting failure 3-68
I/O card failure
troubleshooting 3-69
Input card
fail -DoNotRemove
clear alarm 3-86
mismatch
clear alarm 3-87
missing
clear alarm 3-88
Integrated remote test unit
alarm 1-10
equipment troubleshooting 3-137, 3-158
LED, troubleshooting 7-14
Intercard fail
clear alarm 3-148
Invalid neighbor detected
clear alarm 3-273
IRTU. See Integrated Remote Test Unit
IS 3-48

L

Laser bias current
clear alarm 4-125
LC. See Line Card
LED
access interface card (AIC), troubleshooting 7-12
breaker interface panel, model NT4K14, troubleshooting 7-34
breaker interface panel, model NT7E56, troubleshooting 7-34
circuit pack alarm
clearing 1-1
copper-distribution drawer, troubleshooting 7-7
copper-distribution-shelf power (CDSP), troubleshooting 7-15
driver fail
clearing alarm 3-209

LED (continued)
DS1/VT mapper, troubleshooting 7-27
DS3/STS mapper, troubleshooting 7-28
Epsilon 2-wire station line card (E2WS), troubleshooting 7-16
external synchronization interface (ESI), troubleshooting 7-31
integrated remote test unit (IRTU), troubleshooting 7-14
interpreting 7-1 to 7-34
maintenance interface card (MIC), troubleshooting 7-9
metallic test access card (MTAC), troubleshooting 7-21, 7-22
narrowband line-interface card, troubleshooting 7-20
OC-12, troubleshooting 7-25
OC-3, troubleshooting 7-24
Omega 2-wire office line card (O2WO), troubleshooting 7-18
Omega 2-wire station line card (O2WS), troubleshooting 7-17
Omega 4-wire line card (O4W), troubleshooting 7-19
Omega 6/8-wire line card (O68W), troubleshooting 7-23
OPC tape drive, troubleshooting 7-32
operations controller (OPC), troubleshooting 7-30
processor (Proc), troubleshooting 7-8
status
in-service 7-4
STS-1 interface card, troubleshooting 7-26
test access card (TAC), troubleshooting 7-11
transport interface card (TIC), troubleshooting 7-13
troubleshooting 7-1 to 7-34
LIC. See Line Interface Card
Light-Emitting Diode. See LED
Line card
alarm 1-10
equipment troubleshooting 3-170
Line FE CV threshold
clear alarm 4-70
Line FE ES threshold
clear alarm 4-70
Line FE SES threshold
clear alarm 4-70
Line FE UAS threshold
clear alarm 4-70
Line interface card
alarm 1-11
Line RFI
clear alarm 4-126
Line Rx BCV threshold
clearing alarm 4-163
Line Rx BES threshold
clearing alarm 4-163
Line Rx BSES threshold
clearing alarm 4-163
Line Rx CV threshold
clearing alarm 4-163
Line Rx ES threshold
clearing alarm 4-163
Lockout
protection operation fail
clear alarm 3-241
request
clear alarm 3-89, 3-119, 3-242
protection, clear alarm 3-275
working, clear alarm 3-276
Lockout request
clear alarm 3-339
Loopback
clearing alarm 4-167
Loss of data synchronization
clearing alarm 3-60
lost peer OPC
clear alarm 3-294

M

Maintenance interface card
alarm 1-11
common-equipment circuit pack 2-7
circuit pack fail
alarm 2-7
equipment troubleshooting 3-201
LED, troubleshooting 7-9
operation verification 3-128
Major alarm
BNC I/O card x fail -DoNotRemove 3-112
BNC I/O card x mismatch 3-113

Major alarm (continued)
BNC I/O card x missing 3-114
circuit pack fail 3-43
circuit pack mismatch 3-44
circuit pack missing 3-45
facility provisioning mismatch 3-84, 4-184, 4-203
failure to lock 3-147
input card fail -DoNotRemove 3-86
intercard fail 3-148
major test alarm 3-61
output card fail -DoNotRemove 3-91
prot bridge in card fail -DoNotRemove 3-94
prot bridge out card fail -DoNotRemove 3-97
protection path fail 3-101, 3-121
shelf ID bus fail 3-69
subunit fail 3-149
subunit mismatch 3-150
subunit missing 3-151
test
clear alarm 3-61
timing generation primary reference fail, when both primary and secondary are in alarm status 3-74
traffic problem detected 3-133
using FWALTSCI tool to test generation of 3-61
Major test alarm
clear alarm 3-60
Major, not service-affecting alarm
BNC I/O card x fail -DoNotRemove 3-112
input card fail -DoNotRemove 3-86
major test alarm 3-61
output card fail -DoNotRemove 3-91
prot bridge in card fail -DoNotRemove 3-94
prot bridge out card fail -DoNotRemove 3-97
shelf ID bus fail 3-69
timing generation primary reference fail, when both primary and secondary are in alarm status 3-74
Major, service-affecting alarm
BNC I/O card x
mismatch 3-113
missing 3-114
facility provisioning mismatch 3-84, 4-184, 4-203
Manual switch request
clear alarm 3-90, 3-120
clearing alarm 3-340
releasing 3-90, 3-119, 3-120
Metallic test access card
alarm 1-11
equipment troubleshooting 3-220
LED, troubleshooting 7-21, 7-22
MIC. See Maintenance Interface Card
Minor alarm
autoprovisioning mismatch 3-47
BNC I/O card x fail -DoNotRemove 3-112
circuit pack fail 3-20, 3-43, 3-80, 3-115
circuit pack mismatch 3-21, 3-44, 3-81, 3-116
circuit pack missing 3-22, 3-45, 3-83, 3-117
CNet link fail 3-51
comm overhead clock/frame loss 3-23
comm overhead data loss 3-24
database not restored. Type Q APPROVE at NE 3-54
datasync fail 3-293
D-link interface fail 3-26
equipment forced switch request 3-142, 3-264
equipment lockout request 3-143
equipment manual switch request 3-144
equipment protection switch fail 3-146
exerciser fail 3-59
failure to lock 3-147
forced switch request 3-85, 3-118
input card fail -DoNotRemove 3-86
input card mismatch 3-87
input card missing 3-88
intercard fail 3-148
lockout request 3-89, 3-119
lost peer OPC 3-294
manual switch request 3-90, 3-120
output card fail -DoNotRemove 3-91
output card mismatch 3-92
output card missing 3-93
power filter A missing 3-36

Minor alarm (continued)
power filter B missing 3-39
prot bridge in card fail -DoNotRemove 3-94
prot bridge in card mismatch 3-95
prot bridge in card missing 3-96
prot bridge out card fail -DoNotRemove 3-97
prot bridge out card mismatch 3-98
prot bridge out card missing 3-99
protection path fail 3-101, 3-121
protection switch fail 3-106, 3-126
protection version mismatch 3-110
software trap 3-70
SONET overhead clock loss 3-71
STS1 intercard fail 3-111, 3-129
subunit fail 3-149
subunit mismatch 3-150
subunit missing 3-151
switcher circuit pack mismatch 3-131
switcher circuit pack missing 3-132
tape backup/restore fail 3-309
test 3-62
clearing alarm 3-62
timing generation primary reference fail 3-74
timing generation secondary reference fail 3-74
timing generation secondary reference fail, when both primary and secondary are in alarm status 3-74
T-link interface fail 3-30, 3-31, 3-198
traffic problem detected 3-133
using FWALTSCI tool to test generation of 3-62
VT connection provisioning mismatch 3-136
Minor, not service-affecting alarm
autoprovisioning mismatch 3-47
BNC I/O card x fail -DoNotRemove 3-112
circuit pack fail 3-80
circuit pack mismatch 3-81
circuit pack missing 3-83
CNet link fail 3-51
database not restored. Type Q APPROVE at NE 3-54
Minor, not service-affecting alarm (continued)
equipment forced switch request 3-142, 3-264
equipment lockout request 3-143
equipment manual switch request 3-144
equipment protection switch fail 3-146
exerciser fail 3-59
forced switch request 3-85, 3-118
input card fail -DoNotRemove 3-86
input card mismatch 3-87
input card missing 3-88
lockout request 3-89, 3-119
manual switch request 3-90, 3-120
minor test alarm 3-62
output card fail -DoNotRemove 3-91
output card mismatch 3-92
output card missing 3-93
prot bridge in card fail -DoNotRemove 3-94
prot bridge in card mismatch 3-95
prot bridge in card missing 3-96
prot bridge out card fail -DoNotRemove 3-97
prot bridge out card mismatch 3-98
prot bridge out card missing 3-99
protection switch fail 3-106, 3-126
software trap 3-70
SONET overhead clock loss 3-71
switcher circuit pack mismatch 3-131
switcher circuit pack missing 3-132
timing generation primary reference fail 3-74
timing generation secondary reference fail 3-74
timing generation secondary reference fail, when both primary and secondary are in alarm status 3-74
VT connection provisioning mismatch 3-136
Minor, service-affecting alarm
power filter A missing 3-36
power filter B missing 3-39
MTAC. See Metallic Test Access Card

N

Narrowband line-interface card
  equipment troubleshooting 3-182
  LED, troubleshooting 7-20
Network element
  active alarm list 1-4
  autologout feature 1-2
  ID and name 1-3
  issuing commands locally 2-1
  logout
    communications problems 1-2
  obtaining list of alarms 1-2
  recovering from reload 3-54
  user interface
    obtaining list of alarms 1-2
Network Element Login Manager tool
  alarm clearing 1-3
NT4K2030 shelf identification card failure
  troubleshooting 3-69

O

OC-12
  alarm
    optical interface component failure 2-6
  equipment
    troubleshooting 3-226
    troubleshooting alarms 3-288
  group and slot association 1-15
  interface circuit pack
    LED, troubleshooting 7-25
  transport
    alarm 1-11
OC12. See OC-12 transport
OC-3
  alarm
    optical interface component failure 2-6
  equipment
    troubleshooting 3-226
  group and slot association 1-15
  interface circuit pack
    LED, troubleshooting 7-24
  transport
    alarm 1-11
Omega 2-wire office line card
  LED, troubleshooting 7-18
Omega 2-wire station line card
  LED, troubleshooting 7-17
Omega 4-wire line card
  LED, troubleshooting 7-19
Omega 6/8-wire line card
  LED, troubleshooting 7-23
Operations Controller
  user interface
    obtaining alarm list 1-2
Operations controller
  alarm
    common-equipment circuit pack 2-7
  module
    alarm 1-11
    equipment troubleshooting 3-298
    LED, troubleshooting 7-30
    tape drive, LED, troubleshooting 7-32
  obtaining list
    network element alarms 1-2
  tape backup
    restoring the database 3-55
Optical interface component failure
  alarm 2-6
Optical type 3-50
Optical-laser failure
  alarm 2-6
Output card
  fail -DoNotRemove
    clear alarm 3-91
  mismatch
    clear alarm 3-92
  missing
    clear alarm 3-93

P

p 4-29
Pair gain test controller
  pair gain test controller/metallic test access
      card equipment, troubleshooting 6-1
Parent equipment
  hierarchy 2-8
path Rx CV threshold 1, 2 4-29
Plane A non-operational
  clear alarm 3-63
Plane B non-operational
  clear alarm 3-65

Plane messaging corruption
clearing alarm 3-30, 3-198
Power filter A missing
clear alarm 3-36
Power filter B missing
clear alarm 3-39
Proc. See Processor circuit pack
Processor card
equipment troubleshooting 3-312
LED, troubleshooting 7-8
Processor circuit pack
alarm 1-11
Prot bridge in card
fail -DoNotRemove
clear alarm 3-94
mismatch
clear alarm 3-95
missing
clear alarm 3-96
Prot bridge out card
fail -DoNotRemove
clear alarm 3-97
mismatch
clear alarm 3-98
missing
clear alarm 3-99
Protected configuration
major, service-affecting alarm
intercard fail 3-148
protection path fail 3-101
minor, not service-affecting alarm
circuit pack fail 3-20, 3-43, 3-115
circuit pack mismatch 3-21, 3-44, 3-116
circuit pack missing 3-22, 3-45, 3-117
comm overhead clock/frame loss 3-23
comm overhead data loss 3-24
D-link interface fail 3-26
failure to lock 3-147
protection path fail 3-121
protection version mismatch 3-110
STS1 intercard fail 3-111
subunit fail 3-149
subunit mismatch 3-150
subunit missing 3-151
T-link interface fail 3-30, 3-31, 3-198
traffic problem detected 3-133
Protection groups
manually testing 8-2
Protection path fail
clear alarm 3-101, 3-121
clearing alarm 3-341
Protection switch
complete
clear alarm 3-105, 3-124
clearing alarm 3-344
exerciser failure
troubleshooting 3-121
fail
clear alarm 3-106, 3-126
clearing alarm 3-345
lockout
releasing 3-89
Protection version mismatch
clear alarm 3-110

R

Remote ACO
BIP wirewrap pins 1-5
Ring
protection suspended or unavailable
clear alarm 3-283
reconfiguration in progress
clear alarm 3-67
Rx
clearing alarm
bipolar violation 4-168
line AIS 4-178
loss of frame 4-171
loss of pointer 4-174
loss of signal 4-175
RFI 4-179

S

SDA352 OPC log generation
replacement shelf ID card 3-69
Serial telemetry port failure
alarm 2-7
Shelf alarm monitoring
availability 2-1
Shelf assembly fail
clear alarm 3-68

Shelf ID bus fail
clear alarm 3-69
Side interconnect card failure
troubleshooting 3-68
Software trap
clear alarm 3-70
SONET
clock 3-56
overhead clock loss
clear alarm 3-71
Stratum-3
troubleshooting 3-141
STS-1
facility
troubleshooting 4-163
group and slot association 1-15
I/O card slots 1-16
intercard fail
clear alarm 3-111, 3-129
clearing alarm 3-347
interface card
LED, troubleshooting 7-26
path FE CV threshold 1,2
clearing alarm 4-89
RX AIS
clearing alarm 4-152
RX loss of pointer
clearing alarm 4-156
Rx RFI
clearing alarm 4-93, 4-187
signal label mismatch
clearing alarm 4-57, 4-96
transport 1-10
Subunit
fail
clear alarm 3-149
mismatch, clear alarm 3-150
missing, clear alarm 3-151
Switcher circuit
pack mismatch, clear alarm 3-131
pack mismatch, clearing alarm 3-348
pack missing
clearing alarm 3-349
pack missing, clear alarm 3-132
System diagnostics
failure troubleshooting 3-101

T

TAC. See Test Access Card
tape backup/restore fail
clear alarm 3-309
Tape drive. See Operations controller module, tape drive
TBM shelf
functions
STS-1 circuit pack groups 1-19
Telemetry
latch alarm 2-8
Test access card
alarm 1-11
equipment troubleshooting 3-354
LED, troubleshooting 7-11
Threshold 1 DS0 exceeded
clear alarm 3-34
Threshold 2 DS0 exceeded
clear alarm 3-34
TIC. See Transport Interface Card
Timing generation
entry to acquire
clearing alarm 3-152
primary reference fail
clear alarm 3-73
secondary reference fail
clear alarm 3-73
Timing ref
lockout request
clearing alarm 3-405
prot oscillation control activated
clearing alarm 3-406
prot switch complete
clearing alarm 3-407
prot switch fail
clearing alarm 3-408
T-link interface fail
clear alarm 3-30, 3-31, 3-198
TR-08
frame format 3-110
service
troubleshooting 3-84
traffic
potential loss 3-81

Traffic
problem detected
clear alarm 3-133
upgrade in progress
clear alarm 3-77
Traffic problem detected
clear alarm 3-350
Transport bandwidth manager shelf
functions
DS1 circuit pack groups 1-17
DS3 circuit pack groups 1-18
STS-1 circuit pack groups 1-19
Transport interface card
alarm 1-11
equipment troubleshooting 3-366
facility troubleshooting 4-45, 4-89
failure
troubleshooting 3-63, 3-65
LED, troubleshooting 7-13
switch of activity 3-49
Trbl. See Trouble
Troubleshooting 1-1
B8ZS line coding and AZC alarm encoding 3-84
BNC I/O card ID PROM failure 3-112
CBIC-based card 3-68, 3-69
DS1 input card ID PROM failure 3-86
DS1 output card ID PROM failure 3-91
DS1 protection bridge in card ID PROM failure 3-94
DS1 protection bridge out card ID PROM failure 3-97
DS1 protection hardware failure 3-101
DS1/VT mapper circuit pack failure 3-80
DS1/VT protection mapper mismatch 3-81
external synchronization interface 3-141, 3-142, 3-147, 3-149
facility and equipment problems 3-133
fiber-optic cable connections 3-71
I/O card failure 3-68, 3-69
NT4K2030 shelf identification card 3-69
OC-3/OC-12 optical interface card 3-103
protection switch exerciser failure 3-121
side interconnect card failure 3-68
Stratum-3 3-141
STS1 intercard failure 3-111
system diagnostics failure 3-101
Troubleshooting (continued)
TR-08 service 3-84

U

Unprotected configuration
critical, service-affecting alarm
circuit pack fail 3-20, 3-115
circuit pack mismatch 3-21, 3-116
circuit pack missing 3-22, 3-117
comm overhead clock/frame loss 3-23
comm overhead data loss 3-24
D-link interface fail 3-26
protection version mismatch 3-110
STS1 intercard fail 3-111, 3-129
T-link interface fail 3-30, 3-31, 3-198
major, service-affecting alarm
circuit pack fail 3-43
circuit pack mismatch 3-44
circuit pack missing 3-45
failure to lock 3-147
protection path fail 3-121
subunit fail 3-149
subunit mismatch 3-150
subunit missing 3-151
traffic problem detected 3-133
minor, not service-affecting alarm
intercard fail 3-148
protection path fail 3-101
STS1 intercard fail 3-129
Unused CNet connectors
terminating 3-52

V

VCO. See Voltage Controlled Oscillator
Voltage Controlled Oscillator
troubleshooting 3-141
VT connection provisioning mismatch
clear alarm 3-136

W

Warning
alarm
access failure 3-42
clock failure 3-46
CNet performance degraded 3-52
D-link interface fail 3-26

Warning (continued)
end VCO range 3-141
entry to SONET clock freerun 3-56
equipment protection switch complete 3-145
generation, using FWALTSCI tool 3-78
plane A non-operational 3-63
plane B non-operational 3-65
protection switch complete 3-105, 3-124
traffic upgrade in progress 3-77
warning test alarm 3-78
message
traffic will/may be lost 3-54
not service-affecting alarm
access failure 3-42
clock failure 3-46
CNet performance degraded 3-52
D-link interface fail 3-26
end VCO range 3-141
entry to SONET clock acquire 3-264
entry to SONET clock freerun 3-56
entry to SONET clock holdover 3-266
equipment protection switch complete 3-145
plane A non-operational 3-63
plane B non-operational 3-65
protection switch complete 3-105, 3-124
T-link interface fail 3-30, 3-31
traffic upgrade in progress 3-77
warning test alarm 3-78
test alarm
clear alarm 3-78, 3-80

SONET Products

AccessNode

Alarm and Trouble Clearing Procedures

Copyright © 1993–1999 Nortel Networks, All Rights Reserved.

All information contained in this document is subject to change without notice. Nortel Networks reserves the right to make changes to equipment design or program components, as progress in engineering, manufacturing methods, or other circumstances may warrant.
ACCESSNODE, ACCESSNODE EXPRESS, MAP, NORTEL NETWORKS, and NORTEL are trademarks of Nortel Networks Corporation.
Publication number: 323-3001-543
Document release: Issue 3.0
Date: October 1999

Printed in Canada

NORTEL NETWORKS™