TJ1600 Product Family
6.x Alarm Clearing Procedure

Version: 5.0

Issue Date: 11-Mar-2024

TEJAS® NETWORKS

www.tejasnetworks.com

Warning and Disclaimer

This document is a guide for using Tejas Networks products. While every effort has been made to make this document as complete and as accurate as possible, Tejas Networks does not accept any responsibility for poorly designed or malfunctioning networks. The guide contains Tejas Networks proprietary and confidential information and may not be disclosed, used, or copied without the prior written consent of Tejas Networks or set forth in the applicable license agreement. The information provided in this document is on an "as is" basis and is subject to change without prior notice. The author, Tejas Networks, shall have neither liability nor responsibility to any person or entity with respect to any loss or damage arising from the information contained in this document or from the use of equipment or software that might accompany it. The opinions expressed in this document are not necessarily those of Tejas Networks. The users are solely responsible for the proper use of the software and the application of the results obtained. **TEJAS NETWORKS MAKES NO WARRANTY OR REPRESENTATION, EITHER EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENTATION, ITS QUALITY, PERFORMANCE, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.**

Trademark Acknowledgments

All terms mentioned in this book that are known trademarks or service marks have been appropriately capitalized. All trademarks duly acknowledged. Tejas Networks cannot attest to the accuracy of third-party information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Technical Support Information

Tejas customers can contact Tejas Support Center (TSC) 24x7x365 for any assistance through helpline, fax or email.

- Phone: +91 80 41719090
- Fax: +91 80 26591079
- Email: support@india.tejasnetworks.com
- Skype: tscsupport123
- Web: www.tejasnetworks.com

Additional Learning Resources

The help content for all our products including this content is available online at https://tejdocs.india.tejasnetworks.com/. Please contact our Sales team to get access to this content or to organize any onsite and/or offsite trainings related to our products or technologies.

Feedback

Your opinion is of great value and will help us improve the quality of our documentation and related learning resources. Drop a note to docs@tejasnetworks.com and let us know how we can assist you in your learning.

Revision history

Version	Document ID and issue date	Modifications made
5.0	170-DOC000199-E 11-Mar-2024	Added the following trap IDs in the Equipment alarms section: • Faulty serial link recovery failed - Trap ID: 865 • Fault recovery failed - Trap ID: 866 • Zarlink lock lost - Trap ID: 870 • Serial link configuration in progress - Trap ID: 1133 • Build version mismatch- Trap ID: 1374 • Unknown Ac1200 module inserted: Module new to software - Trap ID: 1412 • File system sanity failure - Trap ID: 1413 • Subtended shelf communication failure - Trap ID: 1414 • Internal error - Trap ID: 1454 Added the following trap IDs in the OTN alarms section: • Local fault - Trap ID: 1403 • Remote fault - Trap ID: 1404 • Continuous APC regulation enabled - Trap ID: 1411
4.0	170-DOC000195-E 17-Nov-2022	Added following alarms: • User password expiry warning – Trap ID: 1362 • User password expired – Trap ID: 1363
3.0	170-DOC000195-E 02-Sep-2022	Added following alarms: • 1359 Remote fault • 1360 Local fault
2.0	170-DOC000188-E 24-Mar-2022	Added Firmware mismatch - Trap ID:1337 and RecoveryFailureWithSecondaryXCCLinks - Trap ID: 1352 alarms in Equipment alarms
1.0	170-DOC000180-E 21-Jul-2021	Standard release

Table of contents

Document overview **11**
Chapter organization 11
Additional resources 11
Target Audience 12
Card protection alarms **13**
Lockout of protection - Trap ID:648 13
Forced Switch to work card - Trap ID:649 13
Manual Switch to work card - Trap ID:650 14
Forced Switch to protect card - Trap ID:651 15
Manual Switch to protect card - Trap ID:652 15
Card Lockout From Protection - Trap ID:653 16
SDH and SONET **17**
Alarm Indication Signal (AIS) on STM/OCn Port - Trap ID:30 17
Alarm Indication Signal (AIS) on AU/STS - Trap ID:352 18
Alarm Indication Signal (AIS) on TU/VT - Trap ID:362 19
Alarm Indication Signal (Terminating) - Trap ID:487 20
APS/MSP Channel mismatch failure - Trap ID:315 21
APS/MSP Mode mismatch failure - Trap ID:314 22
APS/MSP Protect Switch Byte failure - Trap ID:316 23
APS/MSP Far End Protect Line Failure - Trap ID:317 24
BER Threshold exceeded for Signal Degrade - Trap ID:381 25
BER Threshold exceeded on Section for Signal Degrade - Trap ID:480 26
BER Threshold exceeded on Far End Line for Signal Degrade - Trap ID:482 .. 27
BER Threshold Exceeded for Signal Failure (B2) - Trap ID:115 28
BER Threshold Exceeded on Section for Signal Failure - Trap ID:479 29
BER Threshold Exceeded on Far End Line for Signal Failure - Trap ID:481 30
Excessive Error on AU/STS - Trap ID:390 31
Excessive Error on TU/VT - Trap ID:391 32
Far End Excessive Error on AU/STS - Trap ID:484 33
Far End Excessive Error on TU/VT - Trap ID:486 34
Far End Protection Line Failure - Trap ID:444 35
Far End Signal Degrade on AU/STS - Trap ID:483 36
Far End Signal Degrade on TU/VT - Trap ID:485 37
Forced Switch Active - Trap ID:437 38
Lockout Active - Trap ID:436 39
Loss of Frame (LOF) - Trap ID:28 40
Loss of Multiframe on AU/STS - Trap ID:104 41
Loss of Pointer on AU/STS - Trap ID:354 41
Loss of Pointer - Trap ID:364 43
Loss of Signal on STM/OC Port - Trap ID:27 44
Manual Switch Active - Trap ID:438 45
Manual Switch Fail - Trap ID:231 46
Path Label Mismatch on AU/STS - Trap ID:357 47
Path Label Mismatch on TU/VT - Trap ID:367 48
Protection Switch Active - Trap ID:439 49
Protection Channel Match Fail - Trap ID:442 50
Protection mode mismatch - Trap ID:441 51
Protection Switch Byte Fail - Trap ID:443 52

Remote Alarm Indication (RAI) - Trap ID:538 53
Remote Defect Indication - Trap ID:31 54
Remote Defect Indication (RDI) on AU/STS - Trap ID:353 55
Remote Defect Indication (RDI) on TU/VT - Trap ID:363 56
Remote Defect Indication (Terminating) - Trap ID:488 57
Signal Degrade on AU/STS - Trap ID:358 58
Signal Degrade on TU/VT - Trap ID:368 60
Signal Label Unequipped on AU/STS - Trap ID:355 61
Signal Label Unequipped on TU/VT - Trap ID:365 62
Trace Identifier Mismatch on STM/OCn Port - Trap ID:52 63
Trace Identifier Mismatch on AU/STS - Trap ID:356 65
Trace Identifier Mismatch on TU/VT - Trap ID:366 67
Equipment alarms **69**
Address exception on slot - Trap ID: 1236 69
Air Filter Clogged - Trap ID: 1321 69
Bad checksum on configuration file - Trap ID: 7 70
Build version mismatch- Trap ID: 1374 70
Config out of sync - Trap ID:20 71
Card mismatch - Trap ID:153 71
Card Missing - Trap ID:1272 72
Card missing or removed - Trap ID:11 73
Card Unusable - Trap ID:618 73
Circuit Pack Below Baseline - Trap ID:615 74
Cold Restart Required: FPGA Changed - Trap ID:614 75
Communication Link Failure - Trap ID:598 75
Config Downloading - Trap ID:23 76
Configuration missing due to multiple crashes - Trap ID: 1182 77
Database is corrupted/improper - Trap ID:861 77
Database Restore Failed - Trap ID:579 78
Database Save Failed - Trap ID:547 78
Data Path FPGA Erased/UnProgrammed - Trap ID:1320 79
Database write Failure - Trap ID:890 79
DCN Failure - Trap ID:473 80
Derive Voltage High - Trap ID:201 81
Derived Voltage Low - Trap ID:369 81
Dfe re-trigger action failed - Trap ID: 1378 82
External Alarm Occurred - Trap ID:224 82
Factory Defaults Restored - Trap ID:682 83
Fan Failed - Trap ID:434 83
Fault recovery failed - Trap ID: 866 84
Faulty serial link recovery failed - Trap ID: 865 85
File System Almost Full - Trap ID:12 85
File system sanity failure - Trap ID: 1413 86
FPGA Load Failure - Trap ID:18 86
Hardware Failure - Trap ID:13 87
Improper Card Jackin - Trap ID:695 87
Input Voltage High on PSU Card - Trap ID:370 88
Initialization Failure - Trap ID:1068 89
Input Voltage Low On PSU Card - Trap ID:371 89
Intercard communication failure - Trap ID: 378 90
Intercard Suspected - Trap ID:607 91

Internal error - Trap ID: 1454 91
Laser Failure - Trap ID:24 92
LAN Port Down - Trap ID:384 92
Laser power degrading - Trap ID: 887 93
Laser wavelength drifting - Trap ID: 886 94
Laser Temperature High Threshold Crossed - Trap ID:429 94
Laser temperature low threshold crossed - Trap ID:430 95
Laser Supply Voltage High Threshold Crossed - Trap ID:431 95
Laser supply voltage low threshold crossed - Trap ID:432 96
License File not found - Trap ID:1254 97
Memory usage exceeded threshold - Trap ID:116 97
Misconnection Detected on OAM Ports - Trap ID:1092 98
Onboard voltage generation lower threshold crossed - Trap ID:470 98
Onboard voltage generation upper threshold crossed - Trap ID:471 99
PLL program complete -Trap ID: 900 100
Program Fault, Software Failure - Trap ID:15 100
Provisioning Disabled - FileSystem Full - Trap ID:542 100
FirmwareMisMismatch - Trap ID:1337 101
RecoveryFailureWithSecondaryXCCLinks - Trap ID:1352 101
Redundant pair communication failure - Trap ID: 21 102
Routing table near capacity - Trap ID: 685 102
Serial link configuration in progress - Trap ID: 1133 103
SFP failure - Trap ID: 490 103
SFP mismatch - Trap ID: 359 104
SFP missing or removed - Trap ID: 489 105
Shelf disconnected - Trap ID: 1070 106
Software Downloading - Trap ID: 14 106
Stray shelf - Trap ID: 1071 107
Subtended shelf communication failure -Trap ID: 1414 107
Switched off/No input voltage - Trap ID:388 108
Temperature too high - Trap ID: 10 108
Unknown Ac1200 module inserted: Module new to software - Trap ID: 1412 . 109
Zarlink lock lost - Trap ID: 870 109
Facility alarms **111**
ALS Triggered - Laser Is Shutdown - Trap ID:25 111
BacBacBackup Firmware Component is Corrupted - Trap ID:1340 111
Corrupted Active Firmware Component Recovery Failed - Trap ID:1336 112
Excessive Error Ratio - Trap ID:518 113
Firmware version mismatch/invalid with software version - Trap ID:594 113
GCC link failure - Trap ID: 1072 114
Laser Bias current lower threshold crossed - Trap ID:394 115
Laser Bias Current Upper Threshold Crossed - Trap ID:395 115
Line/MS DCC ilnk failure - Trap ID: 597 116
Link Down On Ethernet - Trap ID:305 117
Link Integrity ON - Trap ID:402 117
Lockout Active - Trap ID:436 118
Loopback Active-Facility - Trap ID:377 119
Loopback Active-Terminal - Trap ID:361 120
Loss Average Rx Optical Power - Trap ID:889 121
Manual retry mode - Trap ID: 931 121
NTP Server Unreachable - Trap ID:535 122

Received Power Lower Threshold Crossed - Trap ID:400 122
Received Power upper threshold crossed - Trap ID:401 123
Secondary Reference Out of Range - Trap ID:412 124
Section/RS DCC link failure - Trap ID: 596 124
SFP Auto Provision Mismatch - Trap ID:360 125
SFP Unknown - Trap ID:491 126
Signal Degrade on Ethernet Port - Trap ID:519 126
Transmitted Power Lower Threshold Crossed - Trap ID:392 127
Transmitted Power Upper Threshold Crossed - Trap ID:393 128
MS-SPRing/BLSR Alarms **129**
Invalid K Byte - Trap ID:673 129
Invalid K Byte East - Trap ID:626 129
Invalid K Byte West - Trap ID:627 130
Manual Switch Active on East - Trap ID:632 131
Manual Switch Active On West - Trap ID:634 132
Ring Switch Active - Trap ID:672 133
Ring Switch East - Trap ID:423 134
Ring Switch West - Trap ID:424 135
Security alarms **137**
All Radius Servers are Unavailable - Trap ID:647 137
NE is Enrolled by the NMS/EMS - Trap ID:1206 138
Primary Radius Server Unavailable - Trap ID:645 138
Secondary Radius Servers Unavailable - Trap ID:646 139
User Authentication Failed- Trap ID:320 140
User Password Expiry Warning – Trap ID: 1362 140
User Password Expired – Trap ID: 1363 141
OTN alarms **143**
Alarm Indication Signal on OTU Port - Trap ID:711 143
Alarm Indication Signal - Trap ID:718 143
Alarm Indication Signal on ODU TCM - Trap ID:730 144
Backward Defect Indication - Trap ID:716 145
Backward Defect Indication - Trap ID:723 145
Backward Defect Indication on ODU TCM - Trap ID:760 146
Backward Incoming Alignment Error - Trap ID:713 147
Backward Incoming Alignment Error - Trap ID:761 147
Bridged ODU - Trap ID:880 148
Client Signal Fail - Trap ID:793 149
Client Defect - Trap ID:1126 149
Continuous APC regulation enabled - Trap ID: 1411 150
Degraded Defect on ODU - Trap ID: 722 150
Degraded Defect on ODU TCM - Trap ID: 759 151
Extended Loss Of Frame - Trap ID: 724 151
Extended Loss Of MultiFrame - Trap ID: 725 152
Force Switch Active - Trap ID: 871 153
Force Switch Extra Traffic Signal Active - Trap ID:876 154
Force Switch Null Signal Active - Trap ID:875 154
Incoming Alignment Error - Trap ID:712 155
Incoming Alignment Error on ODU TCM - Trap ID:758 155
Laser is shutdown Due to RPP - Trap ID:1334 156
Local fault - Trap ID: 1403 157
Lockout Active - Trap ID:877 157

Loss of Block Synchronization - Trap ID:1270 158
Locked Defect - Trap ID:719 158
Locked Defect on ODU TCM - Trap ID:731 159
Loss of Frame - Trap ID:709 159
Loss of Frame - Trap ID:1269 160
Loss of MultiFrame - Trap ID:710 161
Loss of Signal - Trap ID:706 162
Loss of Signal - Trap ID:1125 163
Loss of Tandem Connection - Trap ID:762 163
Manual Switch Active - Trap ID:872 164
Manual Switch Null Signal Active - Trap ID:873 165
MultiPlex Structure Identifier Mismatch - Trap ID:728 165
NULL Test Signal - Trap ID:922 166
ODULinearProtection APS bit Mismatch - Trap ID:1123 167
ODULinearProtection Bridged Signal Mismatch - Trap ID:882 167
ODULinearProtection Direction Mismatch - Trap ID:1124 168
ODULinearProtection Freeze Active - Trap ID:884 169
ODULinearProtection Manual Switch Extra Traffic Signal Active - Trap ID:874 169
ODULinearProtection Provision Mismatch - Trap ID:883 170
Open Connection Indication - Trap ID:717 171
Open Connection Indication on ODU TCM - Trap ID:729 171
PayLoad Mismatch - Trap ID:726 172
PRBS Test Signal - Trap ID:921 173
Pre FEC Signal Degrade - Trap ID:1256 173
Remote fault - Trap ID: 1404 174
Selected ODU - Trap ID:881 174
Signal Fail - Trap ID:1128 175
Server Signal Degrade on ODU - Trap ID:721 176
Server Signal Degrade on ODU TCM - Trap ID:705 176
Signal Degrade - Trap ID:714 177
Signal Degrade - Trap ID:1127 177
Server Signal Fail- Trap ID:727 178
Server Signal Fail on ODU TCM - Trap ID:770 178
Trail Trace Identifier Mismatch - Trap ID:715 179
Trail Trace Identifier Mismatch on ODU - Trap ID: 720 180
Trail Trace Identifier Mismatch on ODU TCM - Trap ID:757 180
DWDM alarms **183**
Amplifier Pump Over Current - Trap ID:1073 183
Amplifier Pump High Temperature - Trap ID:1074 183
Amplifier Case Low Temperature - Trap ID: 1075 184
Amplifier Case High Temperature - Trap ID: 1076 184
Amplifier Loss Of Input Power - Trap ID: 1077 185
Amplifier Loss Of Output Power - Trap ID:1078 186
Amplifier High Back Reflection - Trap ID: 1079 187
Amplifier Loss Of Input Power Stage Two - Trap ID: 1080 188
Amplifier Loss Of Output Power Stage Two - Trap ID:1081 189
Amplifier Output Power Out Of Range - Trap ID:1112 190
Amplifier Input Power Out of Range - Trap ID:1113 190
Amplifier Low Input Power - Trap ID:1114 191
Amplifier Degraded Input Power - Trap ID:1115 191
Amplifier Degraded Output Power - Trap ID:1116 192

Amplifier pump over current at stage two - Trap ID:1255 192
APR Triggered - Laser is shutdown - Trap ID:1253 193
Channel Attenuation Out Of Range - Trap ID:1225 194
Channel Power Out Of Range - Trap ID:1226 195
Channel Power Control Failure- Trap ID:1228 195
CFPHwFailure - Trap ID:1322 197
CFPMultiFailure - Trap ID:1324 197
CFPTempFailure - Trap ID:1323 197
Forced Switch Active - Trap ID:1108 198
FPU Lockout of Protection - Trap ID:943 199
FPU Lockout of protection - Trap ID:1259 199
FPU Forced Switch to protect port - Trap ID:944 200
FPU Forced Switch to protect port - Trap ID:1260 200
FPU Forced Switch to work port - Trap ID:945 201
FPU Forced Switch to work port - Trap ID:1261 201
FPU Switched to protect - Trap ID:946 202
Lockout Active - Trap ID:1107 202
Manual Switch Active - Trap ID:1109 203
MSA Module Not Present - Trap ID:1082 204
Pluggable optics Failure - Trap ID:1147 204
Pluggable optics missing or removed - Trap ID:1146 205
Pluggable optics Unknown - Trap ID:1148 206
Pluggable optics Mismatch - Trap ID:1149 207
Protection Switch Active - Trap ID:1110 207
Signal Degrade - Trap ID:1266 208
Signal Fail On Protect - Trap ID:1184 208
Signal Fail On Protect - Trap ID:1262 209
Signal Fail on Work - Trap ID:1185 209
Signal Fail on Work - Trap ID:1263 210
Signal Fail - Trap ID:1227 210
L2 alarms **213**
CCM Interval Mismatch - Trap ID:663 213
Connectivity Check Failed - Trap ID:658 214
FDB Limit Reached - Trap ID:686 214
LAG Capacity Changed- Trap ID: 755 215
LAG Link Down - Trap ID:842 215
Loop Detected - Trap ID:664 216
Loss of Signal - Trap ID:611 217
Misconnection Detected on OAM Ports - Trap ID:1092 217
Multiple RPL Owners Configured - Trap ID:660 218
No RPL Owner Configured - Trap ID:659 218
PacketTrunk OperStatus Down - Trap ID:694 219
Port Mirroring Active - Trap ID:688 219
Remote and Local IP Match - Trap ID:693 220
Remote Defect Indication - Trap ID:662 220
Ringlet External Command Active - Trap ID:1183 221
Traffic Field Mismatch - Trap ID:689 222
Unexpected MAID - Trap ID:661 222
Unexpected MEPID - Trap ID:665 223
Unexpected MD Level - Trap ID:666 223
MPLS-TP Alarms **225**

Misconfiguration of PseudowireGroup-Trap ID: 1175 225
Object creation in hardware failed (Tunnel)-Trap ID: 1173 225
Object creation in hardware failed (Pseudowire)-Trap ID: 1172 226
Protection Switching is Incomplete - Trap ID:669 226
Pseudowire Down (Trap ID: 1132) 227
Remote Defect Indication (Trap ID: 662) 228

1 Document overview

This section describes who must read this guide, how it is organized, and what conventions are used in the document.

1.1 Chapter organization

This document is organized as follows:

Chapter	Scope
Card protection alarms	This chapter describes Card Protection alarms raised on the node and the procedures to clear them.
SDH and SONET	This chapter describes SDH and SONET alarms raised on the node and the procedures to clear them.
Equipment alarms	This chapter describes Equipment alarms raised on the node and the procedures to clear them.
Facility alarms	This chapter describes Facility alarms raised on the node and the procedures to clear them.
Security alarms	This chapter describes Security alarms raised on the node and the procedures to clear them.
OTN alarms	This chapter describes ONT alarms raised on the node and the procedures to clear them.
DWDM alarms	This chapter describes DWDM raised on the node and the procedures to clear them.
L2 alarms	This chapter describes L2 alarms raised on the node and the procedures to clear them.
MPLS-TP Alarms	This chapter describes MPLS-TP alarms raised on the node and the procedures to clear them.

1.2 Additional resources

For more information, refer to the following guides:

Document Name	Description
TJ1600 Product Family 6.x Feature Description Guide V4.0	This document describes the functions, features, capabilities and specification of a product.
TJ1600 Product Family Hardware Description Guide V5.0	This document provides information on hardware configuration, functions, capabilities, limitations, and physical characteristics of the product.

Document Name	Description
TJ1600 Product Family Installation and Commissioning Guide V5.0	This document provides information to install and to initially configure the product to the point of verifying its proper operation in the network.
TJ1600 Product Family 6.x User Interface Guide V5.0	This document introduces and orients service providers to the content, function, and organization of the user interface that support the nodes.
TJ1600 Product Family 6.x L2 User Interface Guide V1.0	This document introduces and orients service providers to the content, function, and organization of the user interface supported on the carrier Ethernet card.

1.3 Target Audience

This document is intended for technicians and maintenance engineers who are responsible for the day-to-day operations of the system.

2 Card protection alarms

This chapter describes card protection alarms raised on Tejas Network Elements and the procedures to clear these alarms.

2.1 Lockout of protection - Trap ID:648

Use this procedure to clear the '*Lockout of protection*' alarm.

Cause

This alarm is raised when the user issues a lockout of protection external command on the protect (protecting) card.

Severity

Minor

Object affected

Card Protection Group

Impact

Card protection for all the Work (Protected) cards becomes unavailable. This alarm is service affecting if the work card fails.

Clearing procedure

To clear this alarm, check for the 'Card Lockout of Protection' alarm and apply **Clear** command.

If the alarm persists, contact your next level of support.

2.2 Forced Switch to work card - Trap ID:649

Use this procedure to clear the '*Forced Switch to work card*' alarm.

Cause

This alarm is raised when user issues Forced Switch to work external command.

Severity

Minor

Object Affected

This alarm is applicable only for protecting card, non-revertive protection and when the protection is active. This alarm is not applicable for 1:N as 1:N is only for revertive mode of operation.

Impact

- Service affecting, if the Work (Protected) card is out of service

- Traffic affecting, if the traffic is on protect card

Clearing Procedure

To clear this alarm, apply the forced switch to work command.

If the alarm persists, contact your next level of support.

2.3 Manual Switch to work card - Trap ID:650

Use this procedure to clear the '*Manual Switch to work card*' alarm.

Cause

This alarm is raised when user issuing Manual Switch to work external command.

Severity

Minor

Object Affected

Card Protection Group

Impact

Traffic affecting, if the traffic is on protect card.

Clearing Procedure

To clear this alarm, apply the Clear or Lockout or Forced Switch commands. Failure of any card involved in work group also clears this alarm.
If the alarm persists, contact your next level of support.

2.4 Forced Switch to protect card - Trap ID:651

Use this procedure to clear the '*Forced Switch to protect card*' alarm.

Cause

This alarm is raised when User issues Forced Switch to protect external command.

Severity

Minor

Object Affected

Card

Impact

Services will be impacted if the protecting card is failed.

Clearing Procedure

To clear this alarm, apply the forced switch to protect command.

If the alarm persists, contact your next level of support.

2.5 Manual Switch to protect card - Trap ID:652

Use this procedure to clear the '*Manual Switch to protect card' alarm.*

Cause

This alarm is raised when the user issues Manual Switch to Protect external command.

Severity

Minor

Object Affected

Card

Impact

The impact of this alarm will be service affecting.

Clearing Procedure

To clear this alarm, apply the Clear or Lockout or Forced Switch commands. Failure of any card involved in Protection group also clears this alarm.

If the alarm persists, contact your next level of support.

2.6 Card Lockout From Protection - Trap ID:653

Use this procedure to clear the '*Card Lockout from protection*' alarm.

Cause

This alarm is raised when user issues a Lockout from protection on the card.

Severity

Minor

Object Affected

Card

Impact

The impact of the alarm is service affecting.

Clearing Procedure

To clear this alarm, apply the Clear of Lockout command.

If the alarm still persists, contact your next level of support.

3 SDH and SONET

3.1 Alarm Indication Signal (AIS) on STM/OCn Port - Trap ID:30

Use this procedure to clear the '*Alarm Indication Signal*' alarm on STM/OCn Port.

Cause

The Alarm Indication Signal *(*AIS) is detected in the K2 byte in the multiplexer section overhead indicating a failure at the far end node. The Alarm Indication Signal on STM/ OCn Port is generated in the downstream nodes.

NOTE: AIS on STMn/OCn Port is not intentionally generated by the network element, however the alarm is reported at the local network element as a consequence of an AIS on the STMn/OCn port existing at the far end network element.

Severity

Critical

Object Affected

STM/OCn Port

Impact

The impacts of this alarm are:

- Traffic affectinagg on unprotected paths.
- Temporary traffic hit if path is switched to the protect path.
- AIS on AU/STS/TU/VT propagated downstream depending on the level of cross connections provisioned.
- RDI on STMn/OCn port propated upstream.

Clearing Procedure

To clear this alarm,

1. Use the network connection information to identify the transmit and receive ends of the alarm signal.
2. Log in to the network element at the transmit end.
3. Retrieve all active alarms from the transmit end.
4. Look for alarm message for the STM/OCn port connected to the local network element. If there is LoS at regenerator level there will be AIS on STMn/OCn port.
5. Clear the alarm using the appropriate procedures.

If the alarm persists, contact your next level of support.

3.2 Alarm Indication Signal (AIS) on AU/STS - Trap ID:352

Use this procedure to clear the '*Alarm Indication Signal*' alarm on AU/STS.

Cause

This alarm is raised when a higher priority alarm such as Loss of Signal, Loss of Frame, MS-AIS, AU/STS-LOP exists on an upstream neighboring node having AU level cross-connects on the same path.

Severity

Major

Object Affected

AU/STS

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Temporary traffic hit if path is switched to the protecting aggregate.
- AIS on AU/STS propagated downstream depending on AU/STS level cross-connects provisioned.
- RDI propagated upstream.

Clearing Procedure

To clear this alarm,

1. Retrieve all active alarms from the local node.
2. Verify if there are alarms of higher order. Clear alarms of higher order on the hierarchy first using the appropriate procedures.
3. Check if 'AIS' alarm on AU/STS is cleared at the local node.
   - If AIS is cleared, the procedure is complete.
   - If AIS persists, go to step 4.
4. Use the network connection information to identify the transmit and receive ends of the alarm signal.
5. Log-in to the node at the transmit end.
6. Retrieve all active alarms from the transmit end.
7. Verify if there are alarms of higher order. Clear alarms of higher order on the hierarchy first using the appropriate procedures.
8. Check if 'AIS' alarm on AU/STS is cleared at the local node.
   - If AIS is cleared, the procedure is complete.
   - If AIS persists, go to step 9.
9. Log into each of the pass-through nodes and retrieve the active alarms.
10. Verify if there are alarms of higher order. Clear alarms of higher order on the hierarchy first using the appropriate procedures.
11. Check if 'AIS' alarm on AU/STS is cleared at the local node.

— If AIS is cleared, the procedure is complete.

If the alarm persists, contact your next level of support.

3.3 Alarm Indication Signal (AIS) on TU/VT - Trap ID:362

Use this procedure to clear the '*Alarm Indication Signal*' alarm on TU/VT.

Cause

This alarm is raised on TU/VT when a higher priority alarm such as Loss of Signal, Loss of Frame, AIS on STM/OCn port/AU/STS/TU/VT, TIM (with TIM action set to downstream AIS) or Signal label mismatch (with Signal label mismatch action set to downstream AIS) exists on an upstream neighboring node.

Severity

Major

Object Affected

TU/VT

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Temporary traffic hit if path is switched to the protecting aggregate.
- AIS on TU/VT or PDH port propagated downstream depending on the level of cross connections provisioned.
- RDI on TU/VT propagated upstream.

Clearing Procedure

To clear this alarm,

1. Retrieve all active alarms from the local node.
2. Verify if there are alarms of higher order. Clear alarms of higher order (Loss of Signal, Loss of frame, AU-LOP, AU-AIS, TU-LOP) on the hierarchy first using the appropriate procedures.
3. Check if 'AIS' alarm on TU/VT is cleared at the near end.
   — If AIS is cleared, the procedure is complete.
   — If AIS persists, go to step 4.
4. Use the network connection information to identify the transmit and receive ends of the alarm signal.
5. Log-in to the node at the transmit end.
6. Retrieve all active alarms from the transmit end.
7. Verify if there are alarms of higher order. Clear alarms of higher order on the hierarchy first using the appropriate procedures.
8. Check if 'AIS' alarm on TU/VT is cleared at the local node.

   - If AIS is cleared, the procedure is complete.
   - If AIS persists, go to step 9.
9. Log into each of the pass-through nodes and retrieve the active alarms.
10. Verify if there are alarms of higher order. Clear alarms of higher order on the hierarchy first using the appropriate procedures.
11. Check if 'AIS' alarm on TU/VT is cleared at the local node.
    - If alarm is cleared, the procedure is complete.

If alarm persists, contact your next level of support.

3.4 Alarm Indication Signal (Terminating) - Trap ID:487

Use this procedure to clear the '*Alarm Indication Signal (Terminating)*' alarm.

Cause

This alarm is raised when:

- there is a higher priority alarm such as Loss of Signal, Loss of Frame, AIS on VT, TIM (with TIM action set to downstream AIS), Signal label mismatch (with Signal label mismatch action set to downstream AIS) exists on an upstream neighboring node.
- on receiving a signal label as Unequipped on the lower or higher order path and the consequent action on receiving Unequipped is set to downstream AIS.

Severity

Major

Object Affected

TU/VT

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Temporary traffic hit if path is switched to the protecting aggregate.
- AIS on TU/VT or PDH port propagated downstream depending on the level of cross connections provisioned.
- RDI on TU/VT propogated upstream.

Clearing Procedure

To clear this alarm,

1. Retrieve all active alarms from the local node.
2. Clear alarms of higher order on the hierarchy first using the appropriate procedures.
3. Check if the alarm is cleared at the near end.

   - If the alarm is cleared, the procedure is complete.
   - If the alarm persists, go to step 4.
4. Use the network connection information to identify the transmit and receive ends of the alarm signal.
5. Log-in to the node at the transmit end.
6. Retrieve all active alarms from the transmit end.
7. Clear alarms of higher order on the hierarchy first using the appropriate procedures.
8. Clear the TIM or PLM alarm on TU/VT at the far end network element with appropriate procedure. If the alarm persists, go to step 9.
9. Check if the '*Alarm Indication Signal (Terminating)*' alarm is cleared at the local node.
10. Log into each of the pass-through network elements and retrieve the active alarms.
11. Verify if there are alarms of higher order. Clear alarms of higher order on the hierarchy first using the appropriate procedures.
12. Check if the alarm is cleared at the local node.
    - If alarm is cleared, the procedure is complete.

If alarm persists, contact your next level of support.

3.5 APS/MSP Channel mismatch failure - Trap ID:315

Use this procedure to clear the '*APS/MSP Channel mismatch failure*' alarm.

Cause

This alarm is raised when the channel number in the received K2 byte is different from that in the transmitted K1 byte. This can happen due to improper fiber connections. This alarm is applicable only if the node is in APS/MSP configuration.

Severity

Minor

Object Affected

APS/MSP Group

Impact

The impact of the alarm is not traffic affecting.

Clearing Procedure

To clear the alarm, ensure that fiber connections are done properly.

If the alarm persists, contact your next level of support.

3.6 APS/MSP Mode mismatch failure - Trap ID:314

Use this procedure to clear the '*APS/MSP Mode mismatch failure*' alarm.

Cause

This alarm is raised when one of the node is configured for bidirectional APS/MSP and the other node is in unidirectional APS/MSP.

Severity

Minor

Object Affected

APS/MSP Group

Impact

Impact of the alarm is non-service affecting.

Clearing Procedure

To clear this alarm,

1. Check the APS/MSP configuration on far end node.
   - If APS/MSP is configured, go to step 3.
   - If APS/MSP is not configured, configure APS/MSP in the far end node. Go to step 4.
2. Ensure that in the far end node and in the near end node, APS/MSP configuration is same, either bidirectional or unidirectional.
3. Check for the '*APS/MSP Mode mismatch failure*' alarm.

— If the alarm is cleared, the procedure is complete.

If the alarm persists. contact your next level of support.

3.7 APS/MSP Protect Switch Byte failure - Trap ID:316

Use this procedure to clear the '*APS/MSP Protect Switch Byte failure*' alarm.

Cause

This alarm is raised when one or more of the following conditions are present in the received K-bytes:

- inconsistent K-bytes
- an invalid, unused, or inappropriate K-byte code
- an invalid or unused channel number

A loss of K-byte continuity between far end and near end nodes may cause this alarm.

NOTE: This alarm is applicable only if the node is in MSP/APS configuration.

Severity

Minor

Object Affected

APS/MSP Group

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

To clear the alarm,

1. Check for the LOS/AIS alarms on the protect port.
   — If alarm is reported, clear the alarms by following the respective trouble clearing procedure. Go to step 3.
   — If alarm is not reported, go to step 2.
2. Check the status of the cards and replace any failed card.
3. Check for the '*APS/MSP Protect Switch Byte failure*' alarm.
   — If alarm is cleared, the procedure is complete.

If the alarm persists, contact your next level of support.

3.8 APS/MSP Far End Protect Line Failure - Trap ID:317

Use this procedure to clear the '*APS/MSP Far End Protection Line failure*' alarm.

Cause

This alarm is raised when the K-byte receives protection line signal failure.

Severity

Minor

Object Affected

APS/MSP Group

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

To clear this alarm,

1. Check the far end alarms on the protection line.
2. Perform the appropriate procedure to clear the alarm at the far end.

If the alarm persists, contact your next level of support.

3.9 BER Threshold exceeded for Signal Degrade - Trap ID:381

Use this procedure to clear the '*BER Threshold exceeded for Signal Degrade*' alarm.

Cause

This alarm is raised on STM/OC port when the bit error ratio (BER) exceeds the set signal degrade (B2) threshold.

The probable causes are:

- faulty fiber or dirty fiber connector.
- faulty transmitter at far end node.
- faulty receiver at local node.
- faulty local node.

Severity

Major

Object Affected

STM/OC port

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Operation status of the associated cross connections degraded.
- Traffic on the respective interface is in error.
- Temporary traffic hit if path switched to protecting one in case of protected cross connections.

Clearing Procedure

To clear this alarm,

1. If the route is protected, ensure that the traffic is switched to the other aggregate port.
2. Clear the fiber bend (if any) and reconnect the fiber properly.
3. Clean the optical fiber.
4. Check if the received power lies in the optimum range. If the received optical power is within the specified range, contact your next level of support.
5. Ensure that there are no damaged fiber connectors or fiber cuts of any kind.
6. Replace the SFP.

If the alarm persists, contact your next level of support.

3.10 BER Threshold exceeded on Section for Signal Degrade - Trap ID:480

Use this procedure to clear the '*BER Threshold exceeded on Section for Signal Degrade*' alarm.

Cause

This alarm is raised on STM/OCn port when the bit error ratio (BER) exceeds the set signal degrade (B1) threshold.

The probable causes are:

- faulty fiber or dirty fiber connector
- faulty transmitter at far end node
- faulty receiver at local node
- faulty local node

Severity

Major

Object Affected

STM/OC Port

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Operation status of the associated cross connections degraded.
- Traffic on the respective interface is in error.
- Temporary traffic hit if path switched to protecting one in case of protected cross connections.

Clearing Procedure

To clear this alarm,

1. If the route is protected, ensure that the traffic is switched to the other aggregate port.
2. Clear the fiber bend (if any) and reconnect the fiber properly.
3. Clean the optical fiber.
4. Check if the received power lies in the optimum range. If the received optical power is within the specified range, contact your next level of support.
5. Ensure that there are no damaged fiber connectors or fiber cuts of any kind.
6. Replace the SFP.

If the alarm persists, contact your next level of support.

3.11 BER Threshold exceeded on Far End Line for Signal Degrade - Trap ID:482

Use this procedure to clear the '*BER Threshold exceeded on Far End Line for Signal Degrade*' alarm.

Cause

This alarm is raised on STM/OCn port when the bit error ratio (BER) exceeds the set signal degrade (B2) threshold.

The probable causes are:

- faulty fiber (uncleaned fiber or fiber bend)
- faulty receiver

Severity

Major

Object Affected

STM/OCn Port

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths
- Operation status of the associated cross connections degraded
- Traffic on the respective interface is in error
- Temporary traffic hit if path switched to protecting one in case of protected cross connections

Clearing procedure

To clear this alarm,

1. If the route is protected, ensure that the traffic is switched to the other aggregate port.
2. Clear the fiber bend (if any) and reconnect the fiber properly.
3. Clean the optical fiber.
4. Check if the received power lies in the optimum range. If the received optical power is within the specified range, contact your next level of support
5. Ensure that there are no damaged fiber connectors or fiber cuts of any kind
6. Replace the SFP.

If the alarm persists, contact your next level of support.

3.12 BER Threshold Exceeded for Signal Failure (B2) - Trap ID:115

Use this procedure to clear the '*BER Threshold Exceeded Signal Failure*' (B2) alarm.

Cause

This alarm is raised on STM/OCn ports when the bit error ratio (BER) exceeds the set signal failure (B2) threshold.

The probable causes are:

- faulty fiber or dirty fiber connector
- faulty transmitter at far end node
- faulty receiver at local node
- faulty local node

Severity

Major

Object Affected

STM/OCn port

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Operation status of the associated cross connections degraded.
- Traffic on the respective interface is in error.
- Temporary traffic hit if path switched to protecting one in case of protected cross connections.

Clearing procedure

To clear this alarm,

1. Ensure that the traffic is switched to the other aggregate port if the route is protected.
2. Clear the fiber bend (if any) and reconnect the fiber properly. Check for 'BER Threshold Exceeded for Signal Failure (B2)' alarm.
3. Clean the optical fiber.
4. If the received power lies in the optimum range, contact your next level of support or else go to step 6.
5. Check if the transmitted power at the far end network element lies in the optimum range.
6. It indicates that SFP is faulty. Replace the SFP at the far end node.

If the alarm persists, contact your next level of support.

3.13 BER Threshold Exceeded on Section for Signal Failure - Trap ID:479

Use this procedure to clear the '*BER Threshold Exceeded on Section for Signal Failure*' (B1) alarm.

Cause

This alarm is raised on STM/OCn ports when the bit error ratio (BER) exceeds the set signal failure (B1) threshold.

The probable causes are:

- faulty fiber or dirty fiber connector
- faulty transmitter at far end node
- faulty receiver at local node
- faulty local node

Severity

Major

Object affected

STM/OCn Port

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths
- Operation status of the associated cross connections degraded
- Traffic on the respective interface is in error
- Temporary traffic hit if path switched to protecting one in case of protected cross connections

Clearing procedure

To clear this alarm,

1. Ensure that the traffic is switched to the other aggregate port if the route is protected.
2. Clear the fiber bend (if any) and reconnect the fiber properly. Check for 'BER Threshold Exceeded on Section for Signal Failure' alarm.
3. Clean the optical fiber.
4. If the received power lies in the optimum range, contact your next level of support or else go to step 6.
5. Check if the transmitted power at the far end network element lies in the optimum range.

6. It indicates that SFP is faulty. Replace the SFP at the far end node.

If the alarm persists, contact your next level of support.

3.14 BER Threshold Exceeded on Far End Line for Signal Failure - Trap ID:481

Use this procedure to clear the '*BER Threshold Exceeded on Far End Line for Signal Failure*' alarm.

Cause

This alarm is raised on STM/OC ports when the bit error ratio (BER) exceeds the set signal failure (B2) threshold.

The probable causes are:

- faulty fib*er (uncleaned fiber or fiber bend)*
- *faulty recei*ver

Severity

Major

Object Affected

STM/OCn port

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths
- Operation status of the associated cross connections degraded
- Traffic on the respective interface is in error
- Temporary traffic hit if path switched to protecting one in case of protected cross connections

Clearing Procedure

To clear this alarm,

1. Ensure that the traffic is switched to the other aggregate port if the route is protected.
2. Clear the fiber bend (if any) and reconnect the fiber properly. Check for 'BER Threshold Exceeded for Signal Failure (B2)' alarm.
3. Clean the optical fiber.
4. If the received power lies in the optimum range, contact your next level of support or else go to step 6.
5. Check if the transmitted power at the far end network element lies in the optimum range.
6. It indicates that SFP is faulty. Replace the SFP at the far end network element.

If the alarm persists, contact your next level of support.

3.15 Excessive Error on AU/STS - Trap ID:390

Use this procedure to clear the '*Excessive Error*' alarm on AU/STS.

Cause

This alarm is raised on AU/STS, when the bit error ratio (BER) of the VC-4 path BIP-8 error rate exceeds the set signal fail (B3) threshold.

The probable causes are:

- faulty fiber or dirty fiber connector
- faulty transmitter at far end node
- faulty receiver at local node

Severity

Major

Object affected

AU/STS

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Operation status of the associated cross connections goes down.
- Traffic on the respective interface is in error.
- Temporary traffic hit if path switched to protecting one in case of protected cross connections.

Clearing procedure

To clear this alarm,

1. Ensure that the traffic is switched to the other aggregate port if the route is protected.
2. Clear the fiber bend (if any) and reconnect the fiber properly. Check for 'Excessive Error on AU (B3)' alarm.
3. Clean the optical fiber.
4. Check if the received power lies in the optimum range. If not, it indicates that SFP is faulty. Replace the SFP.
5. Check if the transmitted power at the far end network element lies in the optimum range. If not, it indicates that SFP is faulty.
6. Replace the SFP at the far end node.

If the alarm persists, contact your next level of support.

3.16 Excessive Error on TU/VT - Trap ID:391

Use this procedure to clear the '*Excessive Error*' alarm on TU/VT.

Cause

This alarm is raised on TU/VT, when the BER of the BIP-2 (VC-12) or BIP-8 (VC-3) error rate exceeds the set signal fail (V5) threshold.

The probable causes are:

- faulty fiber or dirty fiber connector
- faulty transmitter at far end node
- faulty receiver at local node
- faulty local node

Severity

Major

Object Affected

TU/VT

Impact

The impacts of this alarm are:

- traffic affecting on unprotected paths
- Operation status of the associated cross connections degraded
- Traffic on the respective interface is in error
- Temporary traffic hit if path switched to protecting one in case of protected cross connections

Clearing Procedure

To clear this alarm,

1. Ensure that the traffic is switched to the other aggregate port if the route is protected.
2. Clear the fiber bend (if any) and reconnect the fiber properly. Check for 'Excessive Error on TU (V5)' alarm.
3. Clean the optical fiber.
4. Check if the received power lies in the optimum range. If not, it indicates that SFP is faulty. Replace the SFP.

If the alarm persists, contact your next level of support.

3.17 Far End Excessive Error on AU/STS - Trap ID:484

Use this procedure to clear the '*Far End Excessive Error*' alarm.

Cause

This alarm is raised on AU/STS, when the bit error ratio (BER) of the higher order path exceeds the set Signal Fail BER threshold (B3).

The probable causes are:

- faulty fiber (uncleaned fiber or fiber bend)
- faulty receiver

Severity

Major

Object Affected

AU/STS

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Operational status of the associated unprotected cross connections down.
- Traffic on the respective interface in error.
- Temporary traffic hit if path switched to protecting one in case of protected cross connections or MSP/APS protection scheme.

Clearing Procedure

To clear the alarm,

1. If the route is protected, ensure that the traffic is switched to the protecting AU/STS.
2. Clear the fiber bend (if any) and reconnect the fiber properly.
3. Check for 'Far End Excessive Error' alarm.
4. If alarm persists, clean the optical fiber.
5. Check if the 'Far End Excessive Error' alarm is cleared.
6. If alarm persists, check if the received power lies in the optimum range. If the received optical power is not in the specified range. Replace the SFP.
7. Enable ALS at both ends of the optical fiber, if you have disabled it while verifying the Rx power.
8. Check if 'Far End Excessive Error' alarm is cleared.

If the alarm persists, contact your next level of support.

3.18 Far End Excessive Error on TU/VT - Trap ID:486

Use this procedure to clear the '*Far End Excessive Error*' alarm.

Cause

This alarm is raised on the TU/VT object when the bit error ratio (BER) of the lower order path exceeds the set Signal Fail BER threshold (V5).

The probable causes are:

- faulty fiber (uncleaned fiber or fiber bend)
- faulty receiver

Severity

Major

Object Affected

TU/VT

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Operational status of the associated unprotected cross connections down.
- Traffic on the respective interface in error.
- Temporary traffic hit if path switched to protecting one in case of protected cross connections or MSP/APS protection scheme.

Clearing Procedure

To clear the alarm,

1. If the route is protected, ensure that the traffic is switched to the protecting AU/ STS.
2. Clear the fiber bend (if any) and reconnect the fiber properly.
3. Check for 'Far End Excessive Error' alarm.
4. If the alarm persists, clean the optical fiber.
5. Check if the 'Far End Excessive Error' alarm is cleared.
6. If the alarm persists , check if the received power lies in the optimum range. If the received optical power is not in the specified range. Replace the SFP.
7. Enable ALS at both ends of the optical fiber, if you have disabled it while verifying the Rx power.
8. Check if 'Far End Excessive Error' alarm is cleared.

If the alarm persists, contact your next level of support.

3.19 Far End Protection Line Failure - Trap ID:444

Use this procedure to clear the *'Far End Protection Line Fail'* alarm.

Cause

This alarm is raised when the K-byte receives protection line signal failure.

Severity

Major

Object affected

STMn/OCn port

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

To clear this alarm,

1. Check the far end alarms on the protection line.
2. Perform the appropriate procedure to clear the alarm at the far end node.

If the alarm persists, contact your next level of support.

3.20 Far End Signal Degrade on AU/STS - Trap ID:483

Use this procedure to clear the '*Far End Signal Degrade on AU/STS*' alarm

Cause

This alarm is raised when the bit error ratio (BER) of the AU/STS path BIP-8 error rate exceeds the set signal degrade threshold.

The probable causes are:

- faulty fiber (uncleaned fiber or fiber bend)
- faulty receiver

Severity

Major

Object affected

AU/STS

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Operation status of the associated cross connections degraded.
- Traffic on the respective interface is in error.
- Temporary traffic hit if path switched to protecting one in case of protected cross connections.

Clearing procedure

To clear this alarm,

1. If the path is protected, ensure that the traffic is switched to the other aggregate port.
2. Clear the fiber bend (if any) and reconnect the fiber properly.
3. Clean the optical fiber.
4. Check if the received power lies in the optimum range. If yes, contact your next level of support.
5. Ensure that there are no damaged fiber connectors or fiber cuts of any kind.
6. Check if the alarm is cleared at the local node. If not, it indicates that SFP is faulty. Replace the SFP.

If the alarm persists, contact your next level of support.

3.21 Far End Signal Degrade on TU/VT - Trap ID:485

Use this procedure to clear the '*Far End Signal Degrade on TU/VT*' alarm

Cause

This alarm is raised when the bit error ratio (BER) of the TU/VT path BIP-8 error rate exceeds the set signal degrade threshold.

The probable causes are:

- faulty fiber (uncleaned fiber or fiber bend)
- faulty receiver

Severity

Major

Object affected

TU/VT

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths
- Operation status of the associated cross connections degraded
- Traffic on the respective interface is in error
- Temporary traffic hit if path switched to protecting one in case of protected cross connections

Clearing procedure

To clear this alarm,

1. If the path is protected, ensure that the traffic is switched to the other aggregate port.
2. Clear the fiber bend (if any) and reconnect the fiber properly.
3. Clean the optical fiber.
4. Check if the received power lies in the optimum range. If yes, contact your next level of support.
5. Ensure that there are no damaged fiber connectors or fiber cuts of any kind.
6. Check if the alarm is cleared at the local network element. If not, it indicates that SFP is faulty. Replace the SFP.

If the alarm persists, contact your next level of support.

3.22 Forced Switch Active - Trap ID:437

Use this procedure to clear the '*Forced Switch Active*' alarm.

Cause

This alarm is raised on both work and protect channel depending on whether the Force Switch is applied to Work or Protect.

This alarm will be raised on:

- a STM/OCn port, AU/STS, TU/VT, port PDH when User Forced Switch is applied on the port
- AU/STS, TU/VT when User Forced Switch is applied on the corresponding AU/STS port
- any STM/OCn ports (if provisioned as part of a 1+1 MSP/APS), AU/STS and TU/VT (if the STM/OCn port provisioned in SNCP/UPSR mode)

Impact

Traffic will switch to the path to which it is forced to.

Since Signal Fail or Equipment fail on protect is of higher priority, when Forced Switch is applied to Work, the traffic switches back to work.

In MSP/APS, Signal Fail on protect has high priority than Force Switch, so Force Switch to protect will not be allowed to occur.

Severity

Minor

Object affected

- STM/OCn port - Trap ID:437
- Port_PDH - Trap ID:447
- AU/STS - Trap ID:453
- TU/VT - Trap ID:459

Clearing Procedure

To clear this Alarm, apply 'Clear Command' or 'Forced Switch Command' from the node UI.

If the alarm persists, contact your next level of support.

3.23 Lockout Active - Trap ID:436

Use this procedure to clear the '*Lockout Active*' alarm.

Cause

This alarm is raised when a lockout of protection is initiated on an STMn/OCn or PDH ports.

Severity

Minor

Object affected

- TU/VT - Trap ID:458
- AU/STS - Trap ID:452
- Port_PDH - Trap ID:446
- STMn/OCn port - Trap ID:436

Impact

The impact of this alarm can be service affecting if the working channel or port failed. This alarm would be non-service affecting only if traffic is on the work path when the alarm is raised.

Clearing procedure

To clear this alarm,

1. After completion of maintenance, in the node UI go to **Protection** menu and click **Connections** in the navigation menu.
2. Select the connection ID on which the alarm is present and click on **release** button.

If the alarm persists, contact your next level of support.

3.24 Loss of Frame (LOF) - Trap ID:28

Use this procedure to clear the '*Loss of Frame*' alarm on STM/OCn port.

Cause

This alarm is raised when the node detects a severely errored framing generated when the incoming signal has a minimum of twenty four consecutive errored framing patterns.

The probable causes are:

- excessive attenuation
- dirty optical fibers
- dirty connectors
- improper connector seating
- excessive optical power received from the far end
- mismatch in the capabilities (For example, STM-4/16/64 line rate fiber inserted in STM-1 receiver)

Severity

Critical

Object Affected

STM/OCn Port

Impact

The impacts of this alarm are:

- traffic affecting on unprotected paths.
- temporary traffic hit on the protected paths if the paths switched to aggregate containing the alarm.

Clearing Procedure

To clear this alarm on STM/OCn port,

1. Identify the STM/OCn port raising the alarm.
2. Use an up-to-date fiber connection information to identify the transmit and receive sites of the alarm signal.
3. Retrieve all alarms at the transmit end. Clear any alarms of higher order by following the appropriate procedure. Check for the 'Loss of Frame' alarm on local node.
4. Check the Rx power of the receiver to make sure it is above the Rx sensitivity.
5. Ensure that received power at the local node is within the optimum range.
6. Make sure the optical fibers are properly seated in the SFP.
7. If the Rx attenuation is not adjustable, check the transmit power at the far end.
8. If the transmit power is within the Tx specification, the optical attenuation in between the two sites is too high, the optical fiber connections are dirty or the opti-

cal fiber is damaged. Use the appropriate procedure to clean the optical fibers and connectors.
9. Ensure that interfaces connected to each other are of same capacity.
10. Ensure that there is no excessive bend on fibers.
11. Check for the '*Loss Of Frame*' alarm on local node.

If the alarm persists, contact your next level of support.

3.25 Loss of Multiframe on AU/STS - Trap ID:104

Use this procedure to clear '*Loss of Multiframe*' alarm.

Cause

This alarm is raised when:

- the received multiframe number does not match the expected one.
- the network is misconfigured.
- an unprovisioned AU/STS is present on far end network element, which does not send any VCAT overhead to the local node.

Severity

Major

Object affected

AU/STS

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check for misconfiguration in the network.
2. Reconfigure the connections to get the correct configuration.

If the alarm persists, contact your next level of support.

3.26 Loss of Pointer on AU/STS - Trap ID:354

Use this procedure to clear the 'Loss Of Pointer on AU/STS' alarm.

Cause

This alarm is raised on AU/STS if an invalid AU/STS pointer value is received for the three consecutive frames. This condition may arise when:

- there exist a AU/STS mode mismatch between near end and far end network elements. For example, if at near end AU/STS mode is AU4/STS-3 and far end

mode is AU3/STS then AU/STS-LOP will be raised on the second and third AU3/STS of far end equipment

- there is any faulty circuit pack near or far end
- if the cross-connect is present on one end and absent on the other

Severity

Major

Object Affected

AU/STS

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Temporary traffic hit on the protected paths if the paths switched to aggregate containing the alarm.

Clearing Procedure

To clear this alarm,

1. Compare the AU/STS mapping used at the far end node and the local nodet. If there is any mismatch, use the appropriate provisioning procedure to set the proper AU/STS mapping so that the far end and local node uses the same AU/STS mapping
2. Verify if the alarm on AU/STS is cleared at the local node.
3. Ensure that respective cross connects and cards are properly provisioned in the neighboring node.

If the alarm persists, contact your next level of support.

3.27 Loss of Pointer - Trap ID:364

Use this procedure to clear the '*Loss Of Pointer on TU/VT*' alarm.

Cause

This alarm is raised on the TU/VT when:

- there is no cross-connect at the far end network element corresponding to this TU/VT.
- at the far end equipment the tributary circuit pack having PDH/Ethernet ports is not inserted in the node.
- faulty circuit packs at near or far end.

Severity

Major

Object Affected

TU/VT

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Temporary traffic hit on the protected paths if the paths switched to aggregate containing the alarm.

Clearing Procedure

To clear this alarm,

1. Compare the TU/VT mapping used at the far end node and the local node. If there is any mismatch, use the appropriate provisioning procedure to set the proper TU/VT mapping so that the far end and local node uses the same TU/VT mapping.
2. Verify if the alarm on TU/VT is cleared at the local node.
3. Ensure that respective cross connects and cards are properly provisioned in the neighboring node.

If the alarm persists, contact your next level of support.

3.28 Loss of Signal on STM/OC Port - Trap ID:27

Use this procedure to clear the 'Loss of Signal on STMn/OCn port' alarm.

Cause

This alarm is raised on STMn/OCn port when:

- the received optical signal level drops below an determined threshold
- Rx of SFP at the near end or Tx of the SFP at the far end is faulty

Severity

Critical

Object Affected

STM/OCn port

Impact

The impacts of this alarm are:

- Traffic affecting.
- Management connectivity will be lost on that interface.
- Loss of synchronization if network element is locked to that port and the remaining clock switching depends on the nomination of other clock.

Clearing Procedure

To clear this alarm,

1. Check if the received power lies in the optimum range at the local node. If the received optical power is within the specified range, contact your next level of support.
2. Check if the corresponding far end port is admin up. Following appropriate procedures to get the port in admin up condition.
3. Clean the fibers and ensure that there are no fiber cuts.

If the alarm persists, contact your next level of support.

3.29 Manual Switch Active - Trap ID:438

Use this procedure to clear the '*Manual Switch Active*' alarm.

Cause

This alarm is raised only against the work channel when:

- STM/OCn port belonging to an MSP/APS group if Manual switch is applied on it.
- AU/STS/TU/VT channel belonging to SNCP/UPSR pair if manual switch is applied on it.
- Any STM ports (if provisioned as part of a 1+1 MSP), AU and TU (if the STM/OCn port provisioned in SNCP/UPSR mode).

Severity

Minor

Object affected

- TU/VT - Trap ID:460
- AU/STS - Trap ID:454
- Port_PDH - Trap ID:448
- STM/OCn port - Trap ID:438

Impact

Due to this alarm, traffic will be switched to the STM/OCn port or the AU/STS/TU/VT channel to which the manual switch is given. The traffic will stay in the manually switched port or channel until again manually/forcefully switched away from this path or signal failure condition occurs on this path. A traffic outrage of maximum 50 ms. will be experienced on successful manual switching of traffic from one path to another.

Clearing procedure

To clear this Alarm,

1. Use Clear Command or
2. Use Lockout Command or
3. Forced Switch Command or
4. Higher Priority SF/SD Condition.

If the alarm persists, contact your next level of support.

3.30 Manual Switch Fail - Trap ID:231

Use this procedure to clear the 'Manual Switch Fail' alarm.

Cause

This alarm is raised when the last applied external command Manual switch on STM/OC, AU/STS, and TU/VT has failed.

Severity

Warning

Impact

The Manual Switch command applied by the user is not completed by the network element and is ignored.

Object affected

STM/OC, AU/STS, and TU/VT

Clearing procedure

To clear this alarm,

1. Log into the network element web user interface at the default view level with appropriate user access privileges.
2. Determine if there are any alarms present on the interface on which manual switch command is applied. If no alarm is present, contact your next level of support.
3. Use appropriate procedure to clear the alarm.
4. Operate manual switch command again.

3.31 Path Label Mismatch on AU/STS - Trap ID:357

Use this procedure to clear the '*Path label Mismatch*' alarm.

Cause

This alarm is raised on AU/STS, when the received value of the signal label in the C2 byte does not match with the expected signal label value. The probable causes for this alarm are:

- incorrect connection setup.
- incorrect configuration setup.
- faulty local or far end network elements.

Severity

Major

Object Affected

AU/STS

Impact

If generation of downstream AIS on PLM is enabled using profiles, this alarm affects traffic in the following ways:

- Protected traffic will switch to protect path with a hit of maximum 50 ms.
- Unprotected traffic will go down.

Clearing Procedure

To clear this alarm,

1. Retrieve all active alarms on the network element. Clear all the higher alarms using appropriate procedures.
2. Check for appropriate fiber connections. Reconnect the fiber connections to get the right configuration .
3. Check if the values against the Signal Label and Received Signal Label fields match. If mismatch is present, set the transmit same as the received signal label or set the transmit on both the near end and far nodes the same.

Note: The expected signal label is same as the transmitted signal label. There is no field for expected signal label.

If the alarm persists, contact your next level of support.

3.32 Path Label Mismatch on TU/VT - Trap ID:367

Use this procedure to clear the '*Path label Mismatch*' alarm.

Cause

This alarm is raised on TU/VT, when the received value of the signal label in the V5 byte does not match with the expected signal label value. The probable causes for this alarm are:

- incorrect connection setup.
- incorrect configuration setup.
- faulty local or far end nodes

Severity

Major

Object affected

TU/VT

Impact

If generation of downstream AIS on PLM is enabled using profiles, this alarm affects traffic in the following ways:

- protected traffic will switch to protect path with a hit of maximum 50 ms.
- unprotected traffic will go down.

Clearing procedure

To clear this alarm,

1. Retrieve all active alarms on the network element. Clear all the higher alarms using appropriate procedures.
2. Check for appropriate fiber connections. Reconnect the fiber connections to get the right configuration.
3. Check if the values against the Signal Label and Received Signal Label fields match. If mismatch is present, set the transmit same as the received signal label or set the transmit on both the near end and far nodes the same.

Note: The expected signal label is same as the transmitted signal label. There is no field for expected signal label.

If the alarm persists, contact your next level of support.

3.33 Protection Switch Active - Trap ID:439

Use this procedure to clear the '*Protection Switch Active*' alert.

Cause

The alert is raised when traffic is switched from work to protect channel in revertive mode. In case of a bidirectional or an automatic switch, this alert is raised due to:

- a local signal fail
- signal degrade
- loss of frame
- AIS

Severity

Major

Object affected

- STM/OC Port - Trap ID:439
- AU/STS - Trap ID:455
- TU/VT - Trap ID:461
- Port_PDH - Trap ID:449

Impact

The impact of this alert is that traffic is carried in the protect path.

Clearing procedure

To clear this alert,

1. Log into the node UI at the default view level with appropriate user access privileges.
2. Determine if there are any Signal fail or Signal degrade alarm present. Use appropriate procedure to clear the reported alarm.

If the alarm persists, contact your next level of support.

3.34 Protection Channel Match Fail - Trap ID:442

Use this procedure to clear the '*Protection Channel Match Fail*' alarm.

Cause

This alarm is raised when the channel number in the received K2 byte is different from that in the transmitted K1 byte. This can happen due to improper fiber connections. This

alarm is applicable only if the network element is in MSP/APS configuration when NE is in SONET mode.

Severity

Minor

Object affected

STM/OCn port

Impact

The impact of the alarm is non-service affecting.

Clearing procedure

To clear this alarm, ensure that fiber connections are done properly.

If the alarm persists, contact your next level of support.

3.35 Protection mode mismatch - Trap ID:441

Use this procedure to clear the '*Protection mode mismatch*' alarm.

Cause

This alarm is raised when one of the node is configured for bidirectional MSP and the other node is in unidirectional MSP.

Severity

Major

Object Affected

STMn/OCn port

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

To clear this alarm, check the MSP configuration on far end node.

NOTE: All cross-connects on MSP ports have to be deleted before editing the mode of the group.

If MSP/APS is not configured

- Configure MSP/APS in the far end node.
- Ensure that in the far end network element, MSP/APS configuration is bidirectional.

- If MSP/APS is unidirectional, configure the far end node to bidirectional MSP.
- Check for the 'Protection mode mismatch' alarm.

If the alarm persists, contact your next level of support.

If MSP/APS is configured

- Ensure that in the far end network element, MSP/APS configuration is bidirectional.
- If MSP/APS is unidirectional, configure the far end node to bidirectional MSP.
- Check for the 'Protection mode mismatch' alarm.

If the alarm persists, contact your next level of support.

3.36 Protection Switch Byte Fail - Trap ID:443

Use this procedure to clear the '*Protection Switch Byte Fail*' alarm.

Cause

This alarm is raised when one or more of the following conditions are present in the received K-bytes:

- inconsistent K-bytes.
- an invalid, unused, or inappropriate K-byte code.
- an invalid or unused channel number.

A loss of K-byte continuity between far end and near end network elements may cause this alarm.

Severity

Minor

Object Affected

STM/OCn Port

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

To clear this alarm, check for the LOS and AIS alarms on the protect port.

If the LOS and AIS alarms persists:

1. Clear the alarms using the troubleshooting procedures.
2. Check for the 'Protection switch byte fail' alarm if the LOS and AIS alarms are not reported.

If the LOS and AIS alarms are not reported:

1. Check the status of the cards and replace any failed cards.

2. Check for the “Protection switch byte fail” alarm if the LOS and AIS alarms are not reported.

If the alarm persists, contact your next level of support.

Note: If East port of one is connected to east of other node, similarly the West port then Invalid k byte alarm is reported. Now issuing an exerciser command, the command is successfully accepted. The result of 'failure of exerciser' is shown in the events history page. The Invalid K Byte alarm is present but can be any where in the ring.

3.37 Remote Alarm Indication (RAI) - Trap ID:538

Use this procedure to clear the '*Remote Alarm Indication*' alarm.

Cause

This alarm is raised when the receive port of the local network element is receiving RAI from remote PDH port.

Severity

Major

Object affected

Port_PDH

Impact

The impact of the alarm is non-service affecting.

Clearing procedure

To clear this alarm,

1. Check if any alarm exists on the remote PDH port, clear it with appropriate procedure.
2. If the alarm exists, replace the card.

If this alarm persists, contact your next level of support.

3.38 Remote Defect Indication - Trap ID:31

Use this procedure to clear the 'Remote Defect Indication on STMn/OCn Port' alarm.

Cause

This alarm is raised on STMn/OCn port when the byte K2 has been set, indicating that the far end node has detected a fault in the regenerator section/section level or the multiplexer section/line level.

This alarm is reported in case of an LOS, LOF on STMn/OCn port, AIS on STMn/OCn port, TIM with downstream AIS enabled at remote STMn/OCn port of node.

Severity

Critical

Object affected

STM/OCn Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear the alarm,

1. Verify the transmitted and received traces at the STM port (J0 trace) on the far end node.
2. Determine the Rx and Tx directions at the local network element and determine the same on the far end nodes.
3. Login to the far end network element and retrieve a list of alarms. If there are no additional alarms, the equipment and facilities are in-service, then check the fiber else perform the appropriate procedure to clear the alarms.
4. Retrieve the alarms at local node.

If the alarm persists, contact your next level of support.

3.39 Remote Defect Indication (RDI) on AU/STS - Trap ID:353

Use this procedure to clear the 'Remote Defect Indication' alarm on AU/STS.

Cause

This alarm is raised on AU/STS when the fifth bit of the status byte (G1) is set in VC-4/ STS-3/VC-3/STS-1 path, indicating that the downstream node has detected a fault at the higher path level.

This alarm is reported in case of AIS on AU/STS, TIM/PLM with downstream AIS enabled at corresponding remote AU/STS where the higher order path is terminating.

Severity

Major

Object affected

AU/STS

Impact

The Impact of the alarm is non service affecting.

Clearing procedure

To clear this alarm,

1. Determine the Rx and Tx directions at the local network element and determine the same on the far end nodes.
2. Login to the far end node and retrieve a list of alarms.
3. Perform the appropriate procedure to clear the alarms or ensure that the equipment and facilities are in service.
4. Retrieve the alarms at local node. Check if the alarm is cleared at the local node.
5. Verify the fiber connection at far end network element that connects to local node. Repair, clean and reconnect the fiber as required.
6. Retrieve the alarms at local node.

If the alarm persists, contact your next level of support.

3.40 Remote Defect Indication (RDI) on TU/VT - Trap ID:363

Use this procedure to clear the '*Remote Defect Indication on TU/VT*' alarm.

Cause

This alarm is raised on TU/VT when the fifth bit of the status byte (G1/V5 respectively) is set in the VC-3/VC-12 path, indicating that the far end node has detected a fault at the lower path level.

Severity

Major

Object Affected

TU/VT

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

To clear this alarm,

1. Determine the Rx and Tx directions at the local node and determine the same on the far end nodes.
2. Login to the far end node and retrieve a list of alarms.
3. Perform the appropriate procedure to clear the additional alarms
4. Retrieve the alarms at local node. Check if the alarm on TU/VT is cleared at the local node.

If the alarm persists, contact your next level of support.

3.41 Remote Defect Indication (Terminating) - Trap ID:488

Use this procedure to clear the '*Remote Defect Indication on TU/VT*' alarm.

Cause

- This alarm is raised on TU/VT when the fifth bit of the status byte (G1/V5 respectively) is set in VC-3/VC-12, indicating that the far end node has detected a fault at the lower path level.
- This alarm is reported in case of AIS on TU/VT, TIM/PLM with downstream AIS enabled on corresponding remote end TU/VT where the lower order path is terminating.

Severity

Major

Object Affected

TU/VT

Impact

The impact of the alarm is service affecting.

Clearing Procedure

To clear this alarm,

1. Determine the Rx and Tx directions at the local node and determine the same on the far end nodes.
2. Login to the far end node and retrieve a list of alarms.
3. Perform the appropriate procedure to clear the additional alarms.
4. Retrieve the alarms at local node. Check if the alarm on TU/VT is cleared at the local node.

If the alarm persists, contact your next level of support.

3.42 Signal Degrade on AU/STS - Trap ID:358

Use this procedure to clear the '*Signal Degrade*' alarm on AU/STS.

Cause

This alarm is raised when the bit error ratio (BER) of the VC-4 path BIP-8 error rate exceeds the set signal degrade threshold.

The probable causes are:

- faulty fiber or dirty fiber connector
- faulty transmitter at far end node
- faulty receiver at local node
- faulty local node

Severity

Major

Object Affected

AU/STS

Impact

The impacts of this alarm are:

- traffic affecting on unprotected paths.
- operation status of the associated cross connections degraded.
- traffic on the respective interface is in error.
- temporary traffic hit if path switched to protecting one in case of protected cross connections.

Clearing Procedure

To clear this alarm,

1. If the path is protected, ensure that the traffic is switched to the other aggregate port.
2. Determine the port on which alarm is raised. Clear the fiber bend (if any) and reconnect the fiber properly.
3. Check for '*Signal Degrade*' alarm.
   — If the alarm clears, the procedure is complete.
   — If the alarm persists, go to step 4.
4. Clean the optical fiber.
5. Check if the '*Signal Degrade*' alarm is cleared at the local node.
   — If the alarm is cleared, the procedure is complete.
   — If the alarm persists, go to step 6.
6. Check if the received power lies in the optimum range.

- If the received optical power is within the specified range, contact your next level of support.
- If it is not in the specified range, it indicates that SFP/XFP is faulty. Replace the SFP/XFP.

7. Enable ALS at both ends of the optical fiber, if you have disabled the same while verifying the Rx power.
8. Check if '*Signal Degrade*' alarm on AU/STS is cleared at the local node.

— If the alarm is cleared, the procedure is complete.

If the alarm still persists, contact your next level of support.

3.43 Signal Degrade on TU/VT - Trap ID:368

Use this procedure to clear the '*Signal Degrade*' alarm on TU/VT.

Cause

This alarm is raised when the BER of the BIP-2 (VC-12) or BIP-8 (VC-3) error rate exceeds the set signal degrade threshold. The probable causes are:

- faulty fiber or dirty fiber connector
- faulty transmitter at far end node
- faulty receiver at local node
- faulty local node

NOTE: Upon a fiber re-insertion on the STM-N interface, 'Signal Degrade on TU' alarm may be raised. The alarm will clear within a minute.

Severity

Major

Object Affected

TU/VT

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths.
- Operation status of the associated unprotected cross connections degraded.
- Traffic on the respective TU/VT in error.
- Temporary traffic hit if path switched to protecting one in case of protected cross connections.

Clearing Procedure

To clear this alarm,

1. If the path is protected, ensure that the traffic is switched to the other aggregate port.
2. Determine the port on which alarm is raised. Clear the fiber bend (if any) and reconnect the fiber properly.
3. Check for '*Signal Degrade*' alarm.

   - If the alarm clears, the procedure is complete.
   - If the alarm persists, go to step 4.
4. Clean the optical fiber.
5. Check if the '*Signal Degrade*' alarm is cleared at the local node.
   - If the alarm is cleared, the procedure is complete.
   - If the alarm persists, go to step 6.
6. Check if the received power lies in the optimum range.
   - If the received optical power is within the specified range, contact your next level of support.
   - If it is not in the specified range, it indicates that SFP/XFP is faulty. Replace the SFP/XFP.
7. Enable ALS at both ends of the optical fiber, if you have disabled the same while verifying the Rx power.
8. Check if '*Signal Degrade*' alarm on TU/VT is cleared at the local node.
   - If the alarm is cleared, the procedure is complete.

If the alarm still persists, contact your next level of support.

3.44 Signal Label Unequipped on AU/STS - Trap ID:355

Use this procedure to clear the '*Signal Label Unequipped*' alarm on AU/STS.

Cause

This alarm is raised when the Received Signal Label of the corresponding AU/STS is unequipped.

The probable causes for this alarm are:

- probable misconfiguration at the far end upstream node.
- improper provisioning of corresponding cross-connection at one of the far end upstream node.
- improper fiber connections.

Severity

Major

Object Affected

AU/STS

Impact

The impact of the alarm is service affecting.

Clearing Procedure

To clear this alarm,

1. Check the far end upstream node for AU/STS transmit Signal Label (Go to **Facilities>STM/OCn>AU/STS>Signal Label**).

   - If the value of the Signal Label is unequipped, select the appropriate value against the field. Go to step 2.
   - If the value of the Signal Label is any other valid value, contact your next level of support.
2. Ensure that cross-connects are provisioned properly in that particular AU/STS.
3. Ensure proper fiber connections.
4. Check if the '*Signal Label Unequipped*' alarm on AU/STS is cleared at the local node.
   - If the alarm clears, the procedure is complete.
   - If the alarm persists, contact your next level of support.

3.45 Signal Label Unequipped on TU/VT - Trap ID:365

Use this procedure to clear the '*Signal Label Unequipped*' alarm on TU/VT.

Cause

This alarm is raised when the Received Signal Label of the corresponding TU/VT is unequipped.

The probable causes for this alarm are:

- a probable misconfiguration at the far end upstream network element
- improper provisioning of corresponding cross-connection at one of the far end upstream node

Severity

Major

Object Affected

TU/VT

Impact

The alarm is service affecting depending on the consequent action which is set on the particular TU/VT over which the alarm is reported.

Clearing Procedure

To clear this alarm,

1. Ensure that the corresponding cross-connect is properly provisioned.
2. Check at the first upstream node for the '*Signal Label Unequipped*' alarm on TU/VT.
   - If the alarm is reported, go to step 3.
   - If the alarm is not reported, check for the alarm in the consecutive upstream node. Go to step 5.
3. Check for the provisioning of the corresponding cross-connect on upstream node.

— If provisioning is correct, contact your next level of support.
— If provisioning is incorrect, ensure correct provisioning of the cross connection. Go to step 4.

4. Check if the '*Signal Label Unequipped*' alarm on TU/VT is cleared at the local node.
   — If the alarm clears, the procedure is complete.

If the alarm persists, contact your next level of support.

3.46 Trace Identifier Mismatch on STM/OCn Port - Trap ID:52

Use this procedure to clear the '*Trace Identifier Mismatch*' alarm on STMn/OCn Port.

Cause

This alarm is raised when the received string of the trace byte (J0) does not match the expected string.

The probable causes for this alarm are:

- incorrect connection setup.
- incorrect settings during configuration (receive string or far end transmit string).
- faulty local node.

Severity

Major

Object Affected

STM/OCn port

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths depending on the value assigned to the TIM Action field.
- Operation status of the associated unprotected cross connections down.
- Temporary traffic hit if paths switched to protecting one in case of protected cross connections.
- AIS propagated downstream, and RDI propagated upstream when TIM Action field is set to `tim_downstream_ais`.

Clearing Procedure

To clear this alarm,

1. Determine the object on which the alarm is raised.
2. Check if Rx J0 string is same as the Tx J0 string for that object at the far end node connected to the same interface.

- If strings are same, go to step 4.
- If strings are differe

3. nt, then go to 3.
4. Check for the configurations of the node and fiber connectivity.
   - If fiber connections are incorrect, then reconnect to get the right configuration. Go to step 4.
   - If fiber connections are correct, then go to step 4.
5. Reconnect the fiber connections to get the right configuration.
6. Ensure that the values against the **Expected J0** and **Received J0** fields match at the local node.
7. In case of a mismatch detected between the **Transmit J0** at the far end node and **Expected J0** at the local node, correct the same by changing the **Expected J0** value.

NOTE: One byte trace length is supported at the RS level though it has to be numeric rather than an alphabet.

---

8. Check if the '*Trace Identifier Mismatch*' alarm is cleared at the local node.

— If the alarm clears, the procedure is complete.

If the alarm persists, contact your next level of support.

3.47 Trace Identifier Mismatch on AU/STS - Trap ID:356

Use this procedure to clear the '*Trace Identifier Mismatch*' alarm on AU/STS.

Cause

This alarm is raised on AU/STS when the received string of the higher order path trace byte (J1) does not match the expected string.

The probable causes are:

- incorrect connection setup.
- settings incorrect during configuration (receive string or far end transmit string).
- faulty local node.

Severity

Major

Object Affected

AU/STS

Impact

The impacts of this alarm are:

- traffic affecting on unprotected paths depending on the value assigned to the **TIM Action** field
- operation status of the associated unprotected cross connections down.
- temporary traffic hit if paths switched to protecting one in case of protected cross connections.
- AIS propagated downstream, and RDI propagated upstream when **TIM Action** field is set to tim_downstream_ais.

Clearing Procedure

To clear this alarm,

1. Determine the object on which the alarm is raised.
2. Check if Rx J0 string is same as the Tx J0 string for that object at the far end node connected to the same interface.
   — If strings are same, go to step 4.
   — If strings are different, then go to 3.
3. Check for the configurations of the node and fiber connectivity.

- If fiber connections are incorrect, then reconnect to get the right configuration. Go to step 4.
- If fiber connections are correct, then go to step 4.

4. Reconnect the fiber connections to get the right configuration.
5. Ensure that the values against the **Expected J0** and **Received J0** fields match at the local node.
6. In case of a mismatch detected between the **Transmit J0** at the far end node and **Expected J0** at the local node, correct the same by changing the **Expected J0** value.

NOTE: One byte trace length is supported at the RS level though it has to be numeric rather than an alphabet.

---

7. Check if the '*Trace Identifier Mismatch*' alarm is cleared at the local node.

— If the alarm clears, the procedure is complete.

If the alarm persists, contact your next level of support.

3.48 Trace Identifier Mismatch on TU/VT - Trap ID:366

Use this procedure to clear the '*Trace Identifier Mismatch*' alarm on TU/VT.

Cause

This alarm is raised when the received string of the trace byte does not match the expected string.

The probable causes are:

- incorrect connection setup.
- settings incorrect during configuration (receive string or far end transmit string).
- faulty local node.

Severity

Major

Object Affected

TU/VT

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths depending on the value assigned to the **TIM Action** field.
- Operation status of the associated unprotected cross connections down.
- Temporary traffic hit if paths switched to protecting one in case of protected cross connections.
- AIS propagated downstream, and RDI propagated upstream when **TIM Action** field is set to tim_downstream_ais.

Clearing Procedure

To clear this alarm,

Determine the object on which the alarm is raised.

1. Check if Rx J0 string is same as the Tx J0 string for that object at the far end node connected to the same interface.
   — If strings are same, go to step 4.
   — If strings are different, then go to 3.
2. Check for the configurations of the node and fiber connectivity.

- If fiber connections are incorrect, then reconnect to get the right configuration. Go to step 4.
- If fiber connections are correct, then go to step 4.

3. Reconnect the fiber connections to get the right configuration.
4. Ensure that the values against the **Expected J0** and **Received J0** fields match at the local node.
5. In case of a mismatch detected between the **Transmit J0** at the far end node and **Expected J0** at the local node, correct the same by changing the **Expected J0** value.

NOTE: One byte trace length is supported at the RS level though it has to be numeric rather than an alphabet.

---

6. Check if the '*Trace Identifier Mismatch*' alarm is cleared at the local node.
   - If the alarm clears, the procedure is complete.

If the alarm persists, contact your next level of support.

4 Equipment alarms

This chapter describes equipment based alarms raised on Tejas Network Elements and the procedures to clear these alarms.

4.1 Address exception on slot - Trap ID: 1236

Use this procedure to clear the **Address exception on slot** alarm.

Cause

This alarm is raised when the node is unable to access a card in a particular slot.

Severity

Critical

Object affected

Card

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Cold reboot the card.
2. Remove the card and insert it again.
3. If the problem still persists, replace the card.

If the alarm persists, contact your next level of support.

4.2 Air Filter Clogged - Trap ID: 1321

This procedure is used to clear **Air Filter Clogged** alarm.

Cause

Air filter is clogged due to dust particles in the surroundings resulting in blocked airflow to the node. As a reminder to inspect the air filter unit, this alarmed is triggered approximately every 4 months.

Severity

Major

Object Affected

Card

Impact

The impact of the alarm is service affecting.

Clearing Procedure

To clear this alarm, replace the air filter unit.

4.3 Bad checksum on configuration file - Trap ID: 7

Use this procedure to clear the ***Bad checksum on configuration file*** alarm.

Cause

This alarm is raised when the configuration file is modified or corrupt. This is due to improper shutdown/restart of the node software.

Severity

Major

Object Affected

Card

Impact

Traffic will be disrupted and will not be able to write to the configuration file.

Clearing Procedure

To clear this alarm,

1. Restore the configuration file.
2. Reboot the node.

If the alarm persists, contact your next level of support.

4.4 Build version mismatch- Trap ID: 1374

Use this procedure to clear the ***Build version mismatch*** alarm.

Cause

This alarm is raised when there is a mismatch between the build present in the intelligent line card and the build present in the debug path of the intelligent line card.

Severity

Minor

Object affected

Card

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

To clear this alarm, delete the build present in the debug path of the card and give reboot to the card.

If the alarm persists, contact your next level of support.

4.5 Config out of sync - Trap ID:20

Use this procedure to clear the ***Config out of sync*** alarm.

Cause

This alarm is raised when the config file on the two control cards are not in sync.

Severity

Minor

Object Affected

Card

Impact

The impact of the alarm non-service affecting.

Clearing Procedure

To clear this alarm,

1. Ensure the config files on the control cards are same.
2. If not same, do the required upgrade.

If the alarm persists, contact your next level of support.

4.6 Card mismatch - Trap ID:153

Use this procedure to clear the ***Card Mismatch*** alarm.

Cause

This alarm is raised when a slot is provisioned for a specific card and a different card is inserted.

Severity

Major

Object Affected

Card

Impact

The impact of this alarm is as follows:

- The inserted (mismatched) card is not recognized by the node software and is not provisionable.
- The card that is configured initially in the inventory can be used for management operations (for example, port and/or cross connection configuration) but the provisioning changes are not reflected on the hardware and traffic will be down on any provisioned interfaces.

Clearing Procedure

To clear this alarm,

1. Determine the slot against which the alarm is raised.
2. Remove the card from the chassis.
3. In the node UI, delete all objects associated with the card by using **Delete Cards** link on the Node Inventory page.
4. The 'Card mismatch' alarm is cleared and the 'Card missing or removed' alarm is raised.
5. Install the correct card in the slot. The 'Card missing or removed' alarm is cleared.

If the alarm still persists, contact your next level of support.

4.7 Card Missing - Trap ID:1272

Use this procedure to clear ***Card Missing*** alarm.

Cause

This alarm is raised when:

- a slot is provisioned for a specific card and it is not present in the corresponding slot.
- card is not inserted securely to engage the backplane.
- the control card backplane connectors are faulty.
- the backplane is faulty.
- there is pin bends in the card or backplane

Severity

Major

Object Affected

Shelf

Impact

No impact

Clearing Procedure

To clear this alarm,

1. Identify the card that is raising this alarm.
2. Check whether the respective card is inserted properly.
3. Remove the card and re-insert, and check for the alarm.

If the alarm is still present, replace the card with a good card.
4. In case of backplane being faulty, then the cards changing should not be done. If the alarm persists, contact your next level of support.

4.8 Card missing or removed - Trap ID:11

Use this procedure to clear the *Card Missing or Removed* alarm.

Cause

This alarm is raised when:

- a slot is provisioned for a specific card and it is not present in the corresponding slot
- card is not inserted securely to engage the backplane
- the control card backplane connectors are faulty
- the backplane is faulty
- there is pin bends in the card or backplane

Severity

Major

Object Affected

Card

Impact

The impact of the alarm is service affecting.

Clearing Procedure

This alarm is cleared when the appropriate card is installed securely in the slot. To clear this alarm, perform the steps given below:

1. If the card is missing from the provisioned slot, insert the card in the appropriate slot.
2. Verify that the card is inserted securely to engage the backplane.
3. Replace the faulty card.

In case of backplane being faulty, then the cards changing should not be done.

If the problem persists, contact your next level of support.

4.9 Card Unusable - Trap ID:618

Use this procedure to clear the **Card Unusable** alarm.

Cause

This alarm is raised when:

- A tributary protected card is installed without the corresponding IO panel being present in the chassis.
- On the protect card there is no tributary protection group provisioned in the node.

Severity

Major

Object Affected

Card

Impact

Work card will not be usable unless an IO panel is installed and in case of protect card, it will not be usable until it is added to some protection group.

Clearing Procedure

To clear this alarm:

1. Insert the appropriate IO panel required.
2. Check if the alarm is cleared.
3. If alarm persists, create a tributary protection group in the allocated slot.
4. Check if the alarm is cleared.

If the alarm persists, contact your next level of support.

4.10 Circuit Pack Below Baseline - Trap ID:615

Use this procedure to clear the ***Circuit Pack Below Baseline*** alarm.

Cause

This alarm is raised when the card has an older version of the CPLD, which is not supported by the CPLD version of the base card.

Severity

Major

Object Affected

Card

Impact

The impact of the alarm is service affecting.

Clearing Procedure

To clear this alarm,

1. Determine the card against which the alarm is raised.
2. Check the CPLD version of the card.
3. Remove the card against which alarm is raised.
4. Check if the alarm is present. If the alarm persists, contact your next level of support, else move to step 5.
5. Change the CPLD version of the card against which alarm occurred to the version supported by the CPLD version of the base card.

6. Insert the card and check if the alarm is present.

If the alarm persists, contact your next level of support.

4.11 Cold Restart Required: FPGA Changed - Trap ID:614

Use this procedure to clear the ***Cold Restart Required: FPGA Changed*** alarm.

Cause

This alarm is raised during card initialization, if the FPGA version in the current software load is higher than FPGA version on the card. The alarm is also raised over upgrades involving FPGA change but over certain upgrade paths.

Severity

Major

Object Affected

Card

Impact

The impact of the alarm may or may not be service affecting. But cold reboot is service affecting for services on the card.

Clearing Procedure

To clear this alarm, cold reboot the card.

If the alarm persists, contact next level of support.

4.12 Communication Link Failure - Trap ID:598

Use this procedure to clear the **Communication Link Failure** alarm.

Cause

This alarm is raised when the DCC communication has failed on F2, F3, F2F3, E1, or VC12 management channels. This failure may be due to:

- Loss of signal or excessive errors on the optical link
- Loss of signal or excessive errors on the E1 port, in case of E1 management
- DCC not enabled or enabled on a different set of bytes or channels at the remote node
- Remote end node is either faulty or in rebooting stage
- There is a DCN Layer 2 protocol and parameters mismatch between near and far end nodes. For example, near is provisioned for L2 protocol as 'PPP, HDLC Framing' and far end provisioned as 'Standard PPP, RFC 1661'

Note: This failure may be a temporary problem due to the instability of the optical link or remote node and would be corrected when the fault is repaired.

Severity

Major

Object Affected

Network interface

Impact

This alarm is not traffic affecting, but may cause loss of management connectivity to the nodes whose connectivity to the gateway goes through this link, if there is no DCC redundancy.

Clearing Procedure

To clear this alarm:

1. Check for the fiber connectivity by sending trace identifier (J0 byte).
2. Verify the type of management channel being used in the network element. If the management channel type is E1 then ensure that Admin status is up for the E1 port.
3. Ensure that same management channel is used for communication in the neighboring nodes.
4. Check for **Communication Link Failure** on node.

If the alarm persists, contact your next level of support.

4.13 Config Downloading - Trap ID:23

Use this procedure to clear the ***Config Downloading*** alarm.

Cause

This alarm is raised when the command to download config is executed.

Severity

Minor

Object Affected

Card

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

This alarm will be automatically cleared when the Configuration download is completed.

If the alarm persists, contact next level of support.

4.14 Configuration missing due to multiple crashes - Trap ID: 1182

Use this procedure to clear the **Configuration missing due to multiple crashes** alarm.

Cause

This alarm is raised when the node comes up in SLAT mode after multiple crashes with all the configurations deleted.

Severity

Critical

Object affected

Node

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm, restore the configuration.

If the alarm persists, contact your next level of support.

4.15 Database is corrupted/improper - Trap ID:861

Use this procedure to clear the ***Database is corrupted/improper*** alarm.

Cause

This alarm is raised when the network element detects a corrupted configuration file while rebooting or booting the element. This occurs when the checksum calculated on restart does not match the checksum stored previous to the restart.

Severity

Major

Object Affected

Node

Impact

The impact of this alarm is service affecting.

Clearing Procedure

To clear this alarm, perform warm reset to the network element

If the alarm persists, contact your next level of support.

4.16 Database Restore Failed - Trap ID:579

Use this procedure to clear the ***Database Restore Failed*** alarm.

Cause

This alarm is raised when download of configuration database of node has failed.

Severity

Major

Object Affected

Card

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

To clear this alarm,

1. Log-in to the node WUI at the default view level with appropriate user access privileges.
2. Restore the node configuration data successfully.

If the alarm persists, contact your level of support.

4.17 Database Save Failed - Trap ID:547

Use this procedure to clear the ***Database Save Failed*** alarm.

Cause

This alarm is raised when back-up operation of node configuration is failed.

Severity

Major

Object Affected

Card

Impact

The impact of this alarm is non-service affecting.

Clearing Procedure

To clear this alarm,

1. Log-in to the node WUI at the default view level with appropriate user access privileges.
2. Take the successful backup of the node configuration.

If the alarm persists, contact next level of support.

4.18 Data Path FPGA Erased/UnProgrammed - Trap ID:1320

Use this procedure to clear ***Data Path FPGA Erased/UnProgrammed*** alarm.

Cause

Cross-connect FPGA is damaged due to high temperature and due to increased number of objects that increases processing load.

Severity

Major

Object Affected

Card

Impact

The impact of the alarm is service affecting.

Clearing Procedure

To clear this alarm, Cross-connect card level cold reboot/ Cross-connect card Switchover.

4.19 Database write Failure - Trap ID:890

Use this procedure to clear ***Database Write Failure*** alarm.

MIB name

Database write Failure.

Cause

This event is raised when database write/commit operation is failed.

Severity

Critical

Object affected

Card

Impact

The impact of the alarm is non-service affecting.

Clearing procedure

To clear this alarm, correct internally in the software.

If the alarm persists, contact your level of support.

4.20 DCN Failure - Trap ID:473

Use this procedure to clear the ***DCN Failure*** alarm.

Cause

The alarm is raised on the port where In-Band Communication (IBC) is provisioned. This alarm is raised when the IBC or Embedded Communication Channel (ECC) interface is not receiving the packets from the far end node because of:

- higher priority alarm such as Loss of Signal, Loss of Frame, AIS on the STM/OC port existing on the interface
- mismatch in the ECC byte selection between the interfaces at the near end and the far end nodes
- when there is a DCN protocol mismatch existing between the near end and far end nodes

Severity

Major

Object affected

Network Interface

Impact

The impacts of this alarm are as follows:

- Loss of management connectivity over IBC on unprotected paths.
- Temporary loss of management connectivity over IBC on the protected paths.

Clearing procedure

To clear this alarm,

1. Check if there is mismatch in the ECC byte selected on the interfaces, both at the near end and far end nodes.
2. Correct the mismatch, if detected. If the alarm persists, go to step 3.
3. Check for higher priority alarms raised on the STM/OC interface.
4. Perform appropriate procedure to clear the alarms if any. If the alarm persists, go to step 5.
5. Correct the mismatch in DCN protocol at near and far end by ensuring that protocol selected at both ends on the communicating interface is same.

6. Check if the alarm cleared.

If the alarm persists, contact your next level of support.

4.21 Derive Voltage High - Trap ID:201

Use this procedure to clear the ***Derived Voltage High*** alarm.

Cause

This alarm is raised when the onboard voltage has crossed the upper threshold. This could be due to:

- faulty power supply unit
- faulty backplane

Severity

Major

Object affected

Card_PSU

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Determine the card against which the alarm is raised.
2. Replace the faulty card.
3. Check if the alarm is cleared.

If the alarm persists, contact your next level of support.

4.22 Derived Voltage Low - Trap ID:369

Use this procedure to clear the ***Derived Voltage Low*** alarm.

Cause

This alarm is raised when the onboard voltage has gone below the lower threshold. This could be due to:

- faulty power supply unit
- faulty backplane

Severity

Major

Object affected

Card_PSU

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Determine the card against which the alarm is raised.
2. Replace the faulty card with good card.
3. Check whether the alarm cleared.

If the alarm persists, contact your next level of support.

4.23 Dfe re-trigger action failed - Trap ID: 1378

Use this procedure to clear the **Dfe re-trigger action failed** alarm.

Cause

This alarm is raised when there are errors in the XCC serial links after dfe recovery.

Severity

Critical

Object affected

Card

Impact

The impact of this alarm is service affecting and the STM traffic is transmitted with bit errors.

Clearing procedure

To clear this alarm, replace the XCC card and if still the alarm persists then replace the node.

If the alarm persists, contact your next level of support.

4.24 External Alarm Occurred - Trap ID:224

Use this procedure to clear the ***External Alarm Occurred*** alarm.

Cause

This alarm is raised when the external alarm is triggered.

Severity

Critical

Object affected

External alarm

Impact

The impact of the alarm is non-service affecting.

Clearing procedure

To clear this alarm,

1. Check for the cause of the external alarm.
2. Rectify the cause of the external alarm.

If the alarm persists, contact your next level of support.

4.25 Factory Defaults Restored - Trap ID:682

Use this procedure to clear the ***Factory Defaults Restored*** alarm.

Cause

This alarm is raised when you perform a restore factory defaults operation.

Severity

Minor

Object affected

Node

Impact

The impact of this alarm is the objects with previous configuration will be deleted and the traffic will be disrupted.

Clearing procedure

Restore the associated/desired database or proceed with fresh initialization.

If the alarm persists, contact your next level of support.

4.26 Fan Failed - Trap ID:434

Use this procedure to clear the ***Fan Failed*** alarm.

Cause

This alarm is raised when the fan module is not operational. This could be because of:

- Clogged air filter
- Malfunctioning of the fan module or malfunctioning of any of the constituent fans on the fan card

Node supports normal functioning on single fan failure. 'Fan Failed' alarm is raised if at least one fan failure is detected.

Severity

Critical

Object affected

Card

Impact

The impact of this alarm is overheating of the node, which may affect some of the functionalities of the node.

Clearing procedure

To clear this alarm, replace the air filter and/or the fan module.

If there are any visible foreign particles obstructing the fans, remove these particles, replace the air filter and/or the fan module.

The time duration for various chassis variants within which the FTU must be replaced in case of complete FTU failure at an ambient temperature of 40°C:

- 1400-1: 50 sec
- 1400-P: 50 sec
- 1400P-H: 1 min
- 1400-7: 50 sec
- 1400-7 expansion chassis: 50 sec
- 1400-13: 45 sec
- 1400-18: 45 sec

If the alarm persists, contact your next level of support.

4.27 Fault recovery failed - Trap ID: 866

Use this procedure to clear the **Fault recovery failed** alarm.

Cause

This alarm is raised when there is a hardware issue in the line card or the backplane.

Severity

Critical

Object Affected

Card

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm, issue cold reboot to the line card. If the alarm persists after the cold reboot, replace the line card/backplane.

If the alarm still persists, contact your next level of support.

4.28 Faulty serial link recovery failed - Trap ID: 865

Use this procedure to clear the **Faulty serial link recovery failed** alarm.

Cause

This alarm is raised when there is some error in the backplane serial links of the line card even after the automatic serial link reset is done.

Severity

Critical

Object Affected

Card

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm, issue cold reboot to the line card. If the alarm persists after the cold reboot, replace the line card/backplane.

If the alarm still persists, contact your next level of support.

4.29 File System Almost Full - Trap ID:12

Use this procedure to clear the ***File System Almost Full*** alarm.

Cause

This alarm is raised when:

- the free space available is less than 10% of the total disk space.
- disk checking program has detected bad blocks and these blocks may have been marked unusable, thus reducing effective disk space.

Severity

Minor

Object affected

Card

Impact

The impacts of this alarm are:

- non-service affecting

- configuration changes and alarm history may be lost
- any new configuration changes added will not be updated/reflected
- new alarms may not be reliably reported

Clearing procedure

To clear this alarm,

1. Check the disk memory usage.
2. Remove the unwanted files from the disk.
3. Launch the network element user interface session.

If the alarm persists, contact your next level of support.

4.30 File system sanity failure - Trap ID: 1413

Use this procedure to clear the **File system sanity failure** alarm.

Cause

This alarm is raised when there is no read/write access for the controller card's disk.

Severity

Major

Object Affected

Card

Impact

The impact of the alarm is non-service affecting but the node becomes unreachable.

Clearing procedure

To clear this alarm, push the reset button of the controller card or remove and insert the card once.

If the alarm persists, contact your next level of support.

4.31 FPGA Load Failure - Trap ID:18

Use this procedure to clear the ***FPGA Load Failure*** alarm.

Cause

This alarm is raised when the FPGA on card could not be loaded.

Severity

Major

Object Affected

Card

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

To clear this alarm, upgrade with the correct FPGA on the card.

If the alarm persists, contact your next level of support.

4.32 Hardware Failure - Trap ID:13

Use this procedure to clear the ***FPGA Load Failure*** alarm.

Cause

This alarm is raised when:

- there is a hardware problem with the card.
- the backplane is faulty.

Severity

Major

Object affected

Card

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Determine the card against which the alarm is raised.
2. Replace the faulty card securely in the appropriate slot.

If the alarm persists, contact your next level of support.

4.33 Improper Card Jackin - Trap ID:695

Use this procedure to clear the ***Improper Card Jackin*** alarm.

Cause

This alarm is raised when the ejector supported cards have ejectors in unlock state or the card insertion is not proper.

Severity

Major

Object affected

Card

Impact

Card will not be functional. Traffic will be disrupted.

Clearing procedure

To clear this alarm,

1. Remove the card from the chassis.
2. Re-insert the card properly.
3. Push the ejectors to lock state.

If the alarm persists, contact your next level of support.

4.34 Input Voltage High on PSU Card - Trap ID:370

Use this procedure to clear the ***Input Voltage High on PSU Card*** alarm.

Cause

This alarm is raised when the input voltage on PSU exceeds the provisioned voltage high threshold.

Severity

Major

Object affected

Card_PSU

Impact

The impact of this alarm may or may not be traffic affecting, depending on the overload voltage level. A further increase in the input voltage level may result tripping of the PSU and the node will switch off automatically. The node may not switch off if there is redundant power.

Clearing procedure

To clear this alarm:

1. Measure the value of input voltage of the node.
2. Reduce the input voltage to -48V, the ideal input voltage for PSU such that the input voltage to the PSU is well within the normal operating voltage range.
3. The alarm is also cleared when the threshold is increased and within the input voltage range.

If the alarm persists, contact your next level of support.

The following table lists the input voltage range of the TJ1400 products.

Table 1: Input voltage range

Product	Input Voltage Range
DC PSU	
TJ1400-1	-40V DC to -72V DC
TJ1400P-H	-40V DC to -60V DC
TJ1400-7	-40V DC to -72V DC
TJ1400-13	-40V DC to -72V DC
TJ1400-18	-40V DC to -60V DC
AC PSU	
TJ1400-1	100V AC to 240V AC
TJ1400-7	100V AC to 240V AC

4.35 Initialization Failure - Trap ID:1068

Use this procedure to clear ***Initialization Failure*** alarm.

Cause

The alarm is raised when the card has initialization problem. The causes are:

- DDR tunning failure
- System initialization failure

Severity

Major

Object affected

Card

Impact

The impact of the alarm is service affective.

Clearing procedure

To clear this alarm, issue Cold Reboot command to the Card.

If the alarm persists, contact your next level of support.

4.36 Input Voltage Low On PSU Card - Trap ID:371

Use this procedure to clear the ***Input Voltage Low on PSU Card*** alarm.

Cause

This alarm is raised when the input voltage on PSU falls below the provisioned voltage low threshold. The optimum input voltage to the PSU is -48V. The normal operating voltage ranging from -42V to -56V keeps the network element functional.

Severity

Major

Object affected

Card_PSU

Impact

The impact of this alarm may or may not be traffic affecting, depending on the overload voltage level. A further decrease in the input voltage level may result tripping of the PSU and the network element will be switched off automatically. Sometimes node may not switch off if there is redundant power.

Clearing procedure

To clear this alarm:

1. Measure the input voltage of the network element with a voltmeter.
2. Increase the input voltage to -48V, the ideal input voltage for PSU such that the input voltage to the PSU is well within the normal operating voltage range.
3. The alarm is also cleared when the threshold is reduced and within the input voltage range.

If the alarm persists, contact your next level of support.

See the input voltage range listed for TJ1400 products in section **Input Voltage High on PSU Card - Trap ID:370**.

4.37 Intercard communication failure - Trap ID: 378

Use this procedure to clear the **Intercard Communication Failure** alarm.

Cause

This alarm is raised when the processor card is not able to establish connection with the standby card or the intelligent line cards on the Node. This may be due to the rebooting of the other card.

Severity

Major

Object Affected

Card

Impact

This alarm is usually not traffic affecting but may result in traffic outage if protection switch is initiated when this alarm is present on the line cards.

Clearing Procedure

To clear this alarm:

1. Check whether the card on which the alarm is present is inserted properly in the slot.
2. If not, insert the card properly into the slot.
3. Give a warm restart to the node.

If the alarm persists, contact your next level of support.

4.38 Intercard Suspected - Trap ID:607

Use this procedure to clear the ***Intercard Suspected*** alarm.

Cause

This alarm is raised when any of the processor card, Tributary card or the backplane is faulty. For faults which cannot be localized to a particular card, 'Intercard Suspected' alarm will be raised on both the cards: the card on which the failure is reported and the card that generated the failed signal.

Severity

Major

Object affected

Card

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check for the alarm on the faulty card.
2. Replace the faulty card alone.

If the alarm persists, contact your next level of support.

4.39 Internal error - Trap ID: 1454

Use this procedure to clear the **Internal error** alarm.

Cause

This alarm is raised when there is an error in the software of the card.

Severity

Major

Object affected

Card

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm, provide cold reboot to the card or remove the card from the chassis and insert it again.

4.40 Laser Failure - Trap ID:24

Use this procedure to clear the ***Laser Failure*** alarm.

Cause

This alarm is raised when SFP/XFP is faulty.

Severity

Major

Object affected

Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm, replace the SFP/XFP.

If the alarm persists, contact your next level of support.

4.41 LAN Port Down - Trap ID:384

Use this procedure to clear the ***LAN Port Down*** alarm.

Cause

This alarm is raised when:

- LAN Ethernet port is down
- Ethernet cable is disconnected
- Ethernet cable is defective
- Ethernet port on the Ethernet hub, router or switch is down or defective

Severity

Major

Object affected

Network Interface

Impact

If the node is configured as a gateway node, there will be a loss of management connectivity from this node and all nodes managed through this gateway will be unmanageable.

Clearing procedure

To clear this alarm,

1. Check that the LAN cable is connected correctly to the node.
2. Check that the LAN cable is connected correctly to the Ethernet hub/transceiver.
3. If persists, replace the LAN cable.
4. If persists, check that the port on the Ethernet router or switch is enabled and correctly provisioned.
5. Check if the alarm is cleared.

If the alarm still persists, contact your next level of support.

4.42 Laser power degrading - Trap ID: 887

Use this procedure to clear the **Laser power degrading** alarm.

Cause

This alarm is raised when the laser power falls less than the threshold value.

Severity

Major

Object affected

Port

Impact

The impact of this alarm is service affecting.

Clearing procedure

The alarm is cleared when the laser power is within the threshold range.

If the alarm persists, contact your next level of support.

4.43 Laser wavelength drifting - Trap ID: 886

Use this procedure to clear the **Laser wavelength drifting** alarm.

Cause

This alarm is raised when the laser wavelength falls less than the threshold value.

Severity

Major

Object affected

port

Impact

The impact of this alarm is service affecting.

Clearing procedure

The alarm is cleared when the laser wavelength lies within the threshold range.

If the alarm persists, contact your next level of support.

4.44 Laser Temperature High Threshold Crossed - Trap ID:429

Use this procedure to clear ***Laser Temperature High Threshold Crossed*** alarm.

Cause

This alarm is raised when SFP is faulty or Fan module is not working, and the temperature of node itself is too high, it crosses laser temperature high threshold limit (lower temperature limit is -42°C and high temperature 125°C).

Severity Level

Major

Object affected

Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Ensure that environmental temperature is within the operating range of the node.
2. Check for the ***Laser temperature high threshold*** alarm.
   — If the alarm clears, the procedure is complete.

- If the alarm persists, replace the SFP/XFP. Check for the ***Laser temperature high threshold*** alarm.

If the alarm persists, contact your next level of support.

4.45 Laser temperature low threshold crossed - Trap ID:430

Use this procedure to clear the ***Laser temperature low threshold crossed*** alarm.

Cause

This alarm is raised when SFP/XFP is faulty or temperature of the node itself is too low so that it is crossing the lower operational limits of SFP/XFP working.

Severity

Major

Object affected

Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Ensure that environmental temperature is within the operating range of the node.
2. Check for the ***Laser temperature low threshold crossed*** alarm.
   - If the alarm clears, the procedure is complete.
   - If the alarm persists, replace the SFP/XFP. Check for the ***Laser temperature low threshold crossed***' alarm.

If the alarm persists, contact your next level of support.

4.46 Laser Supply Voltage High Threshold Crossed - Trap ID:431

Use this procedure to clear the ***Laser Supply Voltage High Threshold Crossed*** alarm.

Cause

This alarm is raised when the supplied voltage to SFP/XFP module from the on board power supply of the card is higher than high threshold limits.

Severity

Major

Object affected

Port

Impact

The SFP/XFP transmit power may get affected or lead to SFP/XFP failure. The optical receiver on remote system might be damaged, which will affect the traffic.

Clearing procedure

To clear this alarm,

1. Check if ***Laser Supply Voltage High Threshold Crossed*** alarm exists on the cards.
2. If the alarm is reported, clear the alarm by replacing the PSU.
3. Check for the ***Laser Supply Voltage High Threshold Crossed*** alarm again.

If the alarm persists, contact your next level of support.

4.47 Laser supply voltage low threshold crossed - Trap ID:432

Use this procedure to clear the ***Laser supply voltage low threshold*** alarm.

Cause

This alarm is raised when the supplied voltage to SFP/XFP module from the on board power supply of the card is lower than low threshold limits.

Severity

Major

Object affected

Port

Impact

The SFP/XFP transmit power may get affected leading to SFP/XFP failure. LOS may be raised on the remote system, which is traffic affecting.

Clearing procedure

To clear this alarm,

1. Check if ***Laser supply voltage low threshold*** alarm exists on the cards.
2. If the alarm is reported, clear the alarm by replacing the PSU.
3. Check for the ***Laser supply voltage low threshold*** alarm again.

If the alarm persists, contact your next level of support.

4.48 License File not found - Trap ID:1254

Use this procedure to clear ***License File not found*** alarm.

Cause

Alarm is raised indicating the absence of the license file from the node.

Severity

Major

Object affected

Card

Impact

Some features which are dependent on the presence of the license file in the system may not work properly.

Clearing procedure

To clear this alarm,

1. Contact your next level of support to replace the license file in the system.
2. After replacing the license file in the system, Warm reboot has to be given to the node.

If the alarm persists, contact your next level of support.

4.49 Memory usage exceeded threshold - Trap ID:116

Use this procedure to clear the ***Memory usage exceeded threshold*** alarm.

Cause

This alarm is raised when the physical memory (RAM) usage exceeds 90% of the available capacity.

Severity

Minor

Object affected

Card

Impact

Impacts of this alarm are:

- Non-service affecting
- Any new configuration changes will not be updated/reflected

- Performance data will not be updated

Clearing procedure

To clear this alarm,

1. Perform a non-service disruptive reset (warm reboot) on the node.
2. Launch the network element user interface session after the restart.

If the alarm persists, contact your next level of support.

4.50 Misconnection Detected on OAM Ports - Trap ID:1092

Use this procedure to clear ***Misconnection Detected on OAM Ports*** alarm.

Cause

The alarm is raised when loopback is detected on Vlan interface.

Severity

Major

Object affected

System

Impact

The impact of the alarm is no-service affected.

Clearing procedure

To clear this alarm, remove the Loopback on VLAN Interface.

If the alarm persists, contact your next level of support.

4.51 Onboard voltage generation lower threshold crossed - Trap ID:470

Use this procedure to clear the ***Onboard voltage generation lower threshold crossed*** alarm.

Cause

This alarm is raised when the onboard voltage has crossed the lower threshold. This could be due to:

- Faulty card
- Faulty power supply unit
- Faulty backplane

Severity

Major

Object affected

Card

Impact

The impact of this alarm may or may not be traffic affecting, depending on the underload voltage level.

Clearing procedure

To clear this alarm,

1. Determine the card against which the alarm is raised and replace the faulty card.
2. Replace the PSU.

If the alarm persists, contact your next level of support.

4.52 Onboard voltage generation upper threshold crossed - Trap ID:471

Use this procedure to clear the ***Onboard voltage generation upper threshold crossed*** alarm.

Cause

This alarm is raised when the onboard voltage has crossed the upper threshold. This could be due to:

- Faulty card
- Faulty power supply unit
- Faulty backplane

Severity

Major

Object Affected

Card

Impact

Depending on the overload voltage level, the impact of this alarm may or may not be traffic affecting.

Clearing Procedure

To clear this alarm,

1. Determine the card against which the alarm is raised.
2. Replace the faulty card.
3. If the alarm persists, replace the PSU.

If the alarm persists, contact your next level of support.

4.53 PLL program complete -Trap ID: 900

This alarm is not supported in this release.

4.54 Program Fault, Software Failure - Trap ID:15

Use this procedure to clear ***Program Fault, Software Failure*** alarm.

Cause

This alarm is raised when software is unable to open the devices to access.

Severity

Major

Object Affected

Card

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

Reboot the card on which the ***Program Fault, Software Failure*** alarm is raised.

If the alarm persists, contact your next level of support.

4.55 Provisioning Disabled - FileSystem Full - Trap ID:542

Use this procedure to clear the ***Provisioning Disabled - File System Full*** alarm.

Cause

This alarm is raised when the file space on disk is very low.

Severity

Critical

Object affected

Card

Impact

Provisioning is disabled since it can lead to configuration file being deleted or getting corrupt.

Clearing procedure

To clear this alarm, free some space on disk by deleting unnecessary files.

If the alarm persists, contact your next level of support.

4.56 FirmwareMisMismatch - Trap ID:1337

Use this procedure to clear the ***FirmwareMisMismatch*** alarm.

Cause

This alarm is raised when card initialization node detects that firmware version in current software load is not matching version on the device.

Severity

Major

Object affected

AGG2400FabricModule

Impact

The impact of this alarm is that current firmware version on the device is not same as firmware present in the software.

Clearing procedure

To clear this alarm, Cold reboot the card.

4.57 RecoveryFailureWithSecondaryXCCLinks - Trap ID:1352

Use this procedure to clear the ***RecoveryFailureWithSecondaryXCCLinks*** alarm.

Cause

This alarm is raised when the card's backplane serial links with secondary XCC have some errors after reset recovery.

Severity

Critical

Object affected

Card

Impact

Card backplane serial link faulty after reset recovery.

Clearing procedure

If problem persists, replace the card and node.

4.58 Redundant pair communication failure - Trap ID: 21

Use this procedure to clear the **Redundant pair communication failure** alarm.

Cause

This alarm is raised when the redundant card is unable to communicate with the primary card.

Severity

Minor

Object Affected

Card

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

To clear this alarm, check if the primary card is active.

If the alarm persists, contact your next level of support.

4.59 Routing table near capacity - Trap ID: 685

Use this procedure to clear the **Routing table near capacity** alarm.

Cause

This alarm is raised when the **routing database** is high. The calculation of the alarm is dependent on the number of routes present in the system.

Severity

Major

Object Affected

Node

Impact

The impact of this alarm is non-service affecting.

Clearing Procedure

To clear this alarm:

1. Plan the subnet and flood lesser routes to the node.
2. Check the routing table in OSPF through the node.
3. Reduce the number of routes being advertised to the node.

If the alarm persists, contact your next level of support.

4.60 Serial link configuration in progress - Trap ID: 1133

Use this procedure to clear the **Serial link configuration in progress** alarm.

Cause

This alarm is raised when the serial links of the card are under configuration.

Severity

Critical

Object Affected

Card

Impact

The impact of the alarm is service affecting.

Clearing procedure

This alarm is cleared automatically once the serial link configuration is completed.

If the alarm persists, contact your next level of support.

4.61 SFP failure - Trap ID: 490

Use this procedure to clear the **SFP failure** alarm.

Cause

This alarm is raised when a Small Form-factor Pluggable (SFP/XFP) optical transceiver module provisioned on a card fails.

Severity

Critical

Object Affected

SFP

Impact

The impact of the alarm is service affecting.

Clearing Procedure

To clear this alarm:

1. Identify the card and SFP/XFP port raising the alarm.
2. Replace the SFP/XFP optical transceiver module you identified.

If the alarm persists, contact your next level of support.

4.62 SFP mismatch - Trap ID: 359

Use this procedure to clear the **SFP mismatch** alarm.

Cause

This alarm is raised when there is a mismatch in the SFP rate, reach, and wavelength of the inserted SFP/XFP and the expected SFP/XFP.

Severity

Critical

Object Affected

SFP

Impact

This alarm is traffic affecting only if there is a line rate or wavelength mismatch. Traffic is down until you replace the SFP.

Clearing Procedure

To clear this alarm:

1. Determine the SFP/XFP port against which the alarm is raised.
2. Remove the SFP/XFP.
3. Either insert an SFP with the SFP rate, reach, and wavelength as originally provisioned SFP or insert a new SFP that the Tejas node supports.
4. SFP mismatch alarm is also cleared by deleting the SFP from the node inventory.

If the alarm persists, contact your next level of support.

4.63 SFP missing or removed - Trap ID: 489

Use this procedure to clear the **SFP missing or removed** alarm.

Cause

This alarm is raised when the SFP/XFP pluggable is not in the slot.

Severity

Critical

Object Affected

SFP

Impact

This alarm is traffic affecting. Traffic will be down until you replace the SFP/XFP.

Clearing Procedure

To clear this alarm,

1. Insert the appropriate SFP/XFP in the allocated slot.
2. This alarm can also be cleared by deleting the SFP/XFP.

If the alarm persists, contact your next level of support.

4.64 Shelf disconnected - Trap ID: 1070

Use this procedure to clear **Shelf disconnected** alarm.

Cause

This alarm is raised when the subtended shelf is disconnected from the primary node.

Severity

Major

Object affected

Shelf

Impact

The impact of this alarm is non-service affecting.

Clearing procedure

To clear this alarm, reconnect the disconnected node with the primary node.

If the alarm persists, contact your next level of support.

4.65 Software Downloading - Trap ID: 14

This procedure provides information on the **Software Downloading** alarm.

Cause

This alarm is raised in the event of an ongoing software download operation.

Severity

Minor

Object Affected

Card

Impact

The impact of the alarm is non-service affecting.

Clearing Procedure

No action is necessary. This alarm is cleared automatically when the software download operation is complete.

If the alarm persists, contact your next level of support.

4.66 Stray shelf - Trap ID: 1071

Use this procedure to clear the **Stray shelf** alarm.

Cause

This alarm is raised when the primary node is pre-configured with a shelf ID and shelf type but a subtended node with a different shelf type is trying to connect to that shelf ID.

Severity

Major

Object affected

Shelf

Impact

The impact of this alarm is non-service affecting, the shelf connection is not established completely.

Clearing procedure

To clear this alarm, rectify the details of the pre-configured shelf in the primary node.

If the alarm persists, contact your next level of support.

4.67 Subtended shelf communication failure - Trap ID: 1414

Use this procedure to clear the **Zarlink lock lost** alarm.

Cause

This alarm is raised when the master shelf is unable to receive messages from the subtended shelf for 15 minutes.

Severity

Major

Object Affected

Shelf

Impact

The impact of this alarm is non-service affecting but the node becomes unreachable.

Clearing Procedure

To clear this alarm, push the reset button of the controller card present in the subtended shelf or remove and insert the controller card of the subtended shelf once.

If the alarm persists, contact your next level of support.

4.68 Switched off/No input voltage - Trap ID:388

Use this procedure to clear the **Switched off/No input voltage** alarm.

Cause

This alarm is raised when the redundant PSU card is present in the slot but no power is fed to it.

Severity

Major

Object Affected

Card_PSU

Impact

The impact of the alarm is service affecting.

Clearing Procedure

To clear this alarm, feed power to redundant PSU card or suppress the alarm using alarm-filtering method.

To provision Alarm Filter:

1. In the WUI, click **Faults > Alarm Filters** in the navigation pane.
2. Click on **Provision a new alarm filter** and change the following field values:
   - For **Alarm Class**, select the value as **Card.**
   - For **Type**, select the PSU/PFU on which alarm is coming.
   - For **Alarm**, select **Al**l.
   - For **Name**, enter a user defined name.
3. Click on **Create** button.

If the alarm persists, contact your next level of support.

4.69 Temperature too high - Trap ID: 10

Use this procedure to clear the **Temperature too high** alarm.

Cause

This alarm is raised when the temperature of the card exceeds the threshold value.

Severity

Critical

Object affected

Card

Impact

The impact of this alarm is service affecting.

Clearing procedure

This alarm clears automatically when the temperature of the card becomes less than the threshold value.

If the alarm still persists, contact your next level of support.

4.70 Unknown Ac1200 module inserted: Module new to software - Trap ID: 1412

Use this procedure to clear the **Unknown Ac1200 module inserted: Module new to software** alarm.

Cause

This alarm is raised when the AC1200 module of any **Line31/Line32/Line33/line34** card inserted is not known to the software.

Severity

Major

Object Affected

AGG2400FabricModule

Impact

The impact of this alarm is service affecting.

Clearing Procedure

To clear this alarm, upgrade the software of the node to a latest build which supports that AC1200 module.

If the alarm still persists, contact your next level of support.

4.71 Zarlink lock lost - Trap ID: 870

Use this procedure to clear the **Zarlink lock lost** alarm.

Cause

This alarm is raised when the zarlink device present in the card is unable to lock to a reference clock.

Severity

Critical

Object Affected

Card

Impact

The impact of this alarm is service affecting.

Clearing Procedure

To clear this alarm, issue cold reboot to the card. If the alarm persists after the cold reboot, replace the card.

If the alarm still persists, contact your next level of support.

5 Facility alarms

This chapter describes facility based alarms raised on Tejas Network Elements and the procedures to clear these alarms.

5.1 ALS Triggered - Laser Is Shutdown - Trap ID:25

Use this procedure to clear the ***ALS Triggered - Laser is shutdown*** alarm.

Cause

This alarm is raised when there is **Loss of Signal** alarm on a port on which ALS is enabled.

Severity

Major

Object affected

Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check for **Loss of Signal** alarm on near end node.
   - If the alarm is reported, clear the alarm with appropriate procedures and then go to step 3.
   - If the alarm is not reported, contact your next level of support.
2. Check if the **ALS Triggered - Laser is shutdown** alarm is cleared at the local node.
   - If the alarm clears, the procedure is complete.

If the alarm persists, contact your next level of support.

5.2 BacBacBackup Firmware Component is Corrupted - Trap ID:1340

Use this procedure to clear ***Backup Firmware Component is Corrupted*** alarm.

Cause

Alarm indicates the backup firmware component is corrupted and recovery of active firmware component will fail in case active firmware component gets corrupted.

Severity

Critical

Object affected

Card

Impact

The impact of this alarm is service affecting.

Clearing procedure

Repair the backup firmware by using USB.

If the alarm persists, contact your next level of support.

5.3 Corrupted Active Firmware Component Recovery Failed - Trap ID:1336

Use this procedure to clear ***Corrupted Active Firmware Component Recovery Failed*** alarm.

Cause

Alarm indicates the active firmware component is corrupted and recovery from backup firmware component is failed.

This alarm is raised when an active firmware component is corrupted, it can be recovered from backup firmware. There is an option in the node UI to recover the active firmware component.

If the backup firmware also gets corrupted, then the active firmware component cannot be recovered.

Severity

Major

Object affected

Card

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm, recover the corrupted firmware manually through USB.

If the alarm persists, contact your next level of support.

5.4 Excessive Error Ratio - Trap ID:518

Use this procedure to clear the ***Excessive Error Ratio*** alarm.

Cause

This alarm is raised on Ethernet ports when more than 1% of the total frames received at the Ethernet port per second are errored for three consecutive seconds.

This is caused due to:

- Faulty optical cable
- Frames being received that are shorter than the minimum supported frame size of 64 bytes, or frames being received which are longer than the MTU size which is provisioned on the Ethernet port

Severity

Major

Object affected

Ethernet port

Impact

The impacts of this alarm are:

- Traffic affecting on unprotected paths
- Operational status of the associated unprotected cross connections down
- Traffic on the respective interface in error

Clearing procedure

To clear this alarm,

1. Ensure that the Ethernet cable is connected properly.
2. Check if 'Excessive error ratio' alarm on Ethernet port is cleared at the near end node.

If the alarm persists, contact your next level of support.

5.5 Firmware version mismatch/invalid with software version - Trap ID:594

Use this procedure to clear the ***Firmware Version Mismatch/invalid With Software Version*** alarm.

Cause

This alarm is raised when the current firmware version of the network element is not supported by the running software.

Severity

Minor

Object affected

Card

Impact

The impact of this alarm is that some of the features may not be fully functional.

Clearing procedure

To clear this alarm,

1. Upgrade the correct firmware version which is compatible with the existing software.
2. Check for **Firmware Version Mismatch/invalid With Software Version** alarm at the near end.

If the alarm persists, contact your next level of support.

5.6 GCC link failure - Trap ID: 1072

Use this procedure to clear the **GCC link failure** alarm.

Cause

This alarm is raised when,

1. The remote node is faulty or in reboot.
2. GCC is not enabled or different overhead GCC byte is configured on the remote node.
3. There is loss of signal on the optical link.

Severity

Major

Object affected

Network interface

Impact

The impact of this alarm is service affecting only when the GCC link failure is caused due to the loss of signal in the optical link.

Clearing procedure

To clear this alarm,

1. Enable GCC on the remote node and select the correct overhead byte.
2. Check the optical link between the nodes and replace it if there is a link failure.

If the alarm persists, contact your next level of support.

5.7 Laser Bias current lower threshold crossed - Trap ID:394

Use this procedure to clear the ***Laser Bias current lower threshold crossed*** alarm.

Cause

This alarm is raised when the laser bias current goes below the lower threshold of the bias current for the SFP type. This may happen when transmitter is degraded.

Severity

Major

Object affected

Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

1. This alarm will be cleared when the laser bias current is higher than the specified lower threshold value. To clear this alarm, replace the SFP.
2. The alarm is raised when the SFP is freshly jacked in or the port is made admin up. Wait for about a minute, it may get cleared by itself.

If the alarm persists, contact your next level of support.

5.8 Laser Bias Current Upper Threshold Crossed - Trap ID:395

Use this procedure to clear the ***Laser Bias current upper threshold crossed*** alarm.

Cause

This alarm is raised when the laser bias current crosses the upper threshold of the bias voltage for the SFP type. This may happen when:

- the temperature is high
- transmitter has degraded

Severity

Major

Object affected

Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm, replace the SFP.

If the alarm persists, contact your next level of support.

5.9 Line/MS DCC ilnk failure - Trap ID: 597

Use this procedure to clear the **Line/MS DCC Link Failure** alarm.

Cause

This alarm is raised when DCC_M bytes are used on the DCC communication and either of the following condition exists.

- There is LOS/LOF/MS-AIS/Excessive error/Signal degrade alarm on the optical link
- DCC byte is not provisioned on far end
- DCC byte provisioned at far end is other than DCC_M
- There is a DCN Layer 2 protocol and parameters mismatch between near and far end network elements. For example, near is provisioned for L2 protocol as **PPP, HDLC Framing** and far end provisioned as **Standard PPP, RFC 1661** near end network element is faulty
- Far end node is faulty

This may be a temporary problem due to the instability of the optical link or remote node and would be corrected when the fault is repaired.

Severity

Major

Object Affected

Network Interface

Impact

This alarm is non-traffic affecting and may result in the loss of management connectivity to the nodes whose connectivity to the gateway goes through this link, if there is no Line/DCC redundancy.

Clearing Procedure

To clear this alarm:

1. Check for the LOS/LOF/MS-AIS/Excessive error/Signal degrade alarms on the optical interface on which **Line/MS DCC Link Failure** alarm is raised
2. Clear the reported alarm by following the respective trouble clearing procedure or else contact your next level of support
3. Check for **Line/MS DCC Link Failure** alarm on node

4. Check at the far end network element whether DCC byte is provisioned as DCC_M. If DCC byte provisioned at far end node is other than DCC_M, provision it to DCC_M

If the alarm persists, contact your next level of support.

5.10 Link Down On Ethernet - Trap ID:305

Use this procedure to clear the **Link Down on Ethernet** alarm.

Cause

This alarm is raised when:

- there is a faulty connection and/or there is a signal fail at client Ethernet source with link integrity enabled at the local network element
- there is a path break between the local network element and the client Ethernet source due to missing or wrong cross-connections.
- the Auto-negotiation failed between the network element and the client

Severity

Major

Object affected

Data Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check for the alarm on local VCG port. If the alarm is present, go to step 3
2. Ensure that local Ethernet port is admin up
3. Check if the alarm is present on local node
4. Ensure that auto negotiation is enabled on the local node
5. Check for the VCG related alarms on the local node Ethernet port

If the alarm persists, contact your next level of support.

5.11 Link Integrity ON - Trap ID:402

Use this procedure to clear the '*Link Integrity ON*' alarm.

Cause

This alarm is a consequent action on an Ethernet interface whenever the Link Integrity feature is enabled on that interface and an error has occurred on the VCG.

Severity

Major

Object Affected

Ethernet port

Impact

The impact of the alarm is service affecting.

Clearing Procedure

To clear this alarm:

1. Check if the **Link integrity** option in enabled for the Ethernet port of the local node. If link integrity is disabled, contact your next level of support.
2. Check for the admin status of Ethernet port of far end node. If admin status is up, go to step 4.
3. Ensure that port is admin up. Check if the alarm is present on local node. If the alarm persists, go to step 4.
4. Check if **Link down/Auto negotiation failure alarm** present on Ethernet port of far end node. If any of these alarms exist, perform the appropriate procedure to clear the alarm at the far end.
5. Check for the VCG related alarms on the associated local end network element's Ethernet port.

If any alarm persists, contact your next level of support.

5.12 Lockout Active - Trap ID:436

Use this procedure to clear the ***Lockout Active*** alarm.

Cause

This alarm is raised when a lockout of protection is initiated on an STMn/OCn or PDH ports.

Severity

Minor

Object affected

- TU/VT - Trap ID:458
- AU/STS - Trap ID:452
- Port_PDH - Trap ID:446
- STMn/OCn port - Trap ID:436

Impact

The impact of this alarm can be service affecting if the working channel or port failed. This alarm would be non-service affecting only if traffic is on the work path when the alarm is raised.

Clearing procedure

To clear this alarm,

1. After completion of maintenance, in the node UI go to **Protection** menu and click **Connections** in the navigation menu.
2. Select the connection ID on which the alarm is present and click on ***release*** button.

If the alarm persists, contact your next level of support.

5.13 Loopback Active-Facility - Trap ID:377

Use this procedure to clear the ***Loopback Active-Facility*** alarm.

Cause

This alarm is raised when the interface is placed in facility loopback mode through explicit user command.

Severity

Minor

Object affected

Interface

Impact

Due to this alarm, the port will be out of service when facility loopback is active as downstream AIS will be inserted as a result of facility loopback. The loopback has to be removed for the network element to carry the live traffic. Downstream AIS is not inserted on applying facility loopback on DS3 and E3 traffic streams.

Clearing procedure

1. In the node UI, select **Maintenance** in the Navigation menu and click **Loop-Back**. A list of loopback for STMn/OCn, PDH, and Ethernet ports appears.

To clear this alarm on STMn/OCn port,

1. Choose **STMn/OCn.** The corresponding STMn/OCn loopback page appears.
2. Select the STMn/OCn port on which the alarm is raised. The corresponding Port maintenance page appears.
3. Choose **Normal Operation** for the LoopBack Mode and click **Submit.** Click **Accept Valid Modifications.** The **Loopback Active-facility** alarm clears.

If the alarm persists, contact your next level of support.

To clear this alarm on PDH ports,

1. Choose **PDH.** The PDH port loopback page appears.
2. Select the E1/E3/DS1/DS3 port on which the alarm is raised. Corresponding Port maintenance page appears.
3. Choose **Normal Operation** for the LoopBack Mode and click **Submit.** Click **Accept Valid Modifications.** The 'Loopback Active-facility' alarm clears.

If the alarm persists, contact your next level of support.

To clear this alarm on Ethernet ports,

1. Choose **Ethernet.** The Ethernet ports loopback page appears.
2. Select the Ethernet port on which the alarm is raised. The corresponding Port maintenance page appears.
3. Choose **Normal Operation** for the LoopBack Mode and click **Submit.**
4. Click **Accept Valid Modifications.** The **Loopback active-facility** alarm is cleared.

If the alarm persists, contact your next level of support.

5.14 Loopback Active-Terminal - Trap ID:361

Use this procedure to clear the **Loopback Active-Terminal** alarm.

Cause

This alarm is raised when the interface is placed in terminal loopback mode through explicit user command.

Severity

Minor

Object affected

Interface

Impact

The impact of this alarm is that the port will be out of service when the loopback is active. The loopback has to be released in order for the port to carry live traffic.

Clearing procedure

To clear this alarm, select **Maintenance** in the Navigation menu and click **Loop-Back.** A list of loopback for STMn/OCn, PDH/DS1/DS3 and Ethernet ports is displayed.

To clear loopback active-terminal on STMn/OCn ports,

1. Choose **STMn/OCn.** The STMn/OCn port loopback page appears.
2. Select the STMn/OCn port on which the alarm is raised. Corresponding Port maintenance page appears.
3. Choose **Normal Operation** for the LoopBack Mode and click **Submit.**
4. Click **Accept Valid Modifications.** The **Loopback Active-terminal** alarm is cleared.

If the alarm persists, contact your next level of support.

To clear this alarm on PDH ports,

1. Choose **PDH.** The PDH ports loopback page appears.
2. Select the E1/E3/DS1/DS3 port on which the alarm is raised. Corresponding Port maintenance page appears.
3. Choose **Normal Operation** for the LoopBack Mode and click **Submit.**
4. Click **Accept Valid Modifications**. The **Loopback Active-terminal** alarm clears.

If the alarm persists, contact your next level of support.

To clear this alarm on Ethernet ports,

1. Choose **Ethernet.** The Ethernet ports loopback page appears.
2. Select the Ethernet port on which the alarm is raised. Corresponding port maintenance page appears.
3. Choose **Normal Operation** for the LoopBack Mode and click **Submit.**
4. Click **Accept Valid Modifications.** The **Loopback Active-terminal** alarm clears.

If the alarm persists, contact your next level of support.

5.15 Loss Average Rx Optical Power - Trap ID:889

Use this procedure to clear ***Loss Average Rx Optical Power*** alarm.

Cause

Alarm is raised for tunable optics. It indicates a loss of receive power for the tuned wavelength.

Severity

Major

Object affected

Port

Impact

The impact of the alarm causes protected traffic to switch away from the port and unprotected traffic might be impacted.

Clearing procedure

Check whether laser power is in normal range. If yes, then check the fiber path in the network and identify the source of the low power and correct the same.

If the alarm persists, contact your next level of support.

5.16 Manual retry mode - Trap ID: 931

Use this procedure to clear the **Manual retry mode** alarm.

Cause

This alarm is raised when the manual retry button appears on the reroute path page due to the absence of the reroute path.

Severity

Critical

Object affected

GMPLS circuit

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm, click on the manual retry option.

If the alarm persists, contact your next level of support.

5.17 NTP Server Unreachable - Trap ID:535

Use this procedure to clear the ***NTP Server Unreachable*** alarm.

Cause

This alarm is raised when the node is not synchronized with the NTP server.

Severity

Minor

Object affected

Node

Impact

The impact of this alarm is node will not be synchronized with NTP server.

Clearing procedure

To clear this alarm,

1. Ensure that NTP server is provisioned properly.
2. Ensure that NTP server is reachable from the node.
3. Check if the alarm is cleared at the near end.

If the alarm persists, contact your next level of support.

5.18 Received Power Lower Threshold Crossed - Trap ID:400

Use this procedure to clear the ***Received Power lower threshold crossed*** alarm.

Cause

This alarm is raised when the received power drops below the lower threshold power for the SFP type which is used in the network element. This alarm will be cleared when the received power is more than the specified lower threshold value.

Severity

Major

Object affected

Port

Impact

The impact of this alarm may or may not be traffic affecting, depending on the lower received power level.

Clearing procedure

To clear this alarm,

1. Check for the received power level. If the received power is low, check the fiber channel.
2. Clean and replace the fiber.
3. Replace the SFP on the far end node.

If the alarm persists, contact your next level of support.

5.19 Received Power upper threshold crossed - Trap ID:401

Use this procedure to clear the ***Received Power upper threshold crossed*** alarm.

Cause

This alarm is raised when the received power crosses the upper threshold power for the SFP type which is used in the network element. This can be due to:

- higher transmitting power of the upstream network element
- very little optical attenuation between the two network element

This alarm will be cleared when the received power is less than the specified upper threshold value.

Severity

Major

Object affected

Port

Impact

The impact of this alarm may or may not be traffic affecting, depending on the upper received power level.

Clearing procedure

To clear this alarm,

1. Check for the received power level. If it is higher, introduce proper attenuation.
2. If the alarm is not cleared, replace the SFP in the remote node.

If the alarm persists, contact your next level of support.

5.20 Secondary Reference Out of Range - Trap ID:412

Use this procedure to clear the ***Secondary Reference out of range*** alarm.

Cause

This alarm is raised when secondary reference goes out of lock because of very high frequency difference.

Severity

Major

Object affected

Synchronization

Impact

If primary fails synchronization does not work, secondary is out of reference.

Clearing procedure

No action is required. It gets settled by itself after some time.

If the alarm persists, contact your next level of support.

5.21 Section/RS DCC link failure - Trap ID: 596

Use this procedure to clear the **Section/RS DCC link failure** alarm.

Cause

This alarm is raised when DCC_R bytes are used on the DCC communication and one of the following conditions exists:

- There is an LOS/LOF/MS-AIS/Excessive error alarm on the optical link
- DCC byte is not provisioned on far end
- DCC byte provisioned at far end is other than DCC_R

- if there is a mismatch in Layer 2 or OSPF parameters. For example, near is provisioned for L2 protocol as **PPP, HDLC Framing** and far end is provisioned as **Standard PPP, RFC 1661**
- Near end node is faulty
- Far end node is faulty

Severity

Major

Object Affected

Network Interface

Impact

The impact of this alarm is loss of management connectivity over IBC (Inband Communication).

Clearing Procedure

To clear this alarm:

1. Check for the LOS/LOF/MS-AIS/Excessive error/Signal degrade alarm on the optical interface on which **Section/RS DCC Link Failure** alarm is raised.
   — If any alarm is reported, clear the alarm using appropriate clearing procedure. Go to step 2.
   — If any alarm is not reported, contact your next level of support.
2. Check for the **Section/RS DCC Link Failure** alarm on the node.
   — If the alarm clears, the procedure is complete.
   — If the alarm persists, go to step 3.
3. Check at the far end node whether DCC byte is provisioned as DCC_R.
   — If is provisioned other than DCC_R, provision it to DDC_R. Ensure that DCN protocol provisioned at both Near and far end network elements are same. Go to step 4.
   — If DCC byte provisioned at far end network element is same as that in the near end node, contact your next level of support.
4. Check for **Section/RS DCC Link Failure** alarm on node.
   — If the alarm clears, the procedure is complete.

If the alarm persists, contact your next level of support.

5.22 SFP Auto Provision Mismatch - Trap ID:360

Use this procedure to clear the ***SFP Auto Provision Mismatch*** alarm.

Cause

This alarm is raised when there is a mismatch in the port capacity and the laser capacity of the SFP/XFP.

Severity

Critical

Object affected

SFP/XFP

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Make sure that there is no traffic through the node and then remove the SFP/XFP.
2. Delete the SFP/XFP object.
3. Insert a new SFP/XFP with the laser capacity same as the port capacity.
4. Check if the **SFP Auto Provision Mismatch** alarm is cleared at the local node.
   — If the alarm clears, the procedure is complete.

If the alarm persists, contact your next level of support.

5.23 SFP Unknown - Trap ID:491

Use this procedure to clear the ***SFP Unknown*** alarm.

Cause

This alarm is raised when the SFP pluggable is from a non approved vendor.

Severity

Critical

Object affected

SFP

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Unplug the unapproved SFP.
2. Delete the entry of SFP.
3. Plug-in any approved SFP.

If the alarm persists, contact your next level of support.

5.24 Signal Degrade on Ethernet Port - Trap ID:519

Use this procedure to clear the ***Signal Degrade*** alarm on Ethernet Ports.

Cause

This alarm is raised on Ethernet ports when more than 1% of the total frames received at the Ethernet port per second are errored for three consecutive seconds. The probable causes are:

- faulty optical cable
- received frame size is smaller/larger than the supported frame size

Severity

Minor

Object affected

Ethernet Port

Impact

The impact of the alarms is service affecting.

Clearing procedure

To clear this alarm,

1. Ensure that the Ethernet cable is connected properly.
2. Ensure that the MTU size of the data is within the supported range.
3. Check if **Signal Degrade** alarm on Ethernet port is cleared at the local node.
   — If the alarm clears, the procedure is complete.

If the alarm persists, contact your next level of support.

5.25 Transmitted Power Lower Threshold Crossed - Trap ID:392

Use this procedure to clear the **Transmitted Power lower threshold crossed** alarm.

Cause

This alarm is raised when the transmitted power drops below the lower threshold power for the SFP/XFP transceiver which is used for the node. This alarm will be cleared when the transmitted power is more than the specified lower threshold value. This alarm is also raised if ALS is enabled on a port and LOS is present on Rx port.

Severity

Major

Object affected

Port

Impact

This alarm may affect traffic if the transmitted power level has crossed the lower threshold considerably.

Clearing procedure

To clear this alarm,

1. This alarm indicates that SFP/XFP of the local network element is faulty. Replace the faulty SFP/XFP with an equivalent one.
2. Check if the **Transmitted Power lower threshold crossed** alarm is cleared at the local node.

If the alarm persists, contact your next level of support.

5.26 Transmitted Power Upper Threshold Crossed - Trap ID:393

Use this procedure to clear the ***Transmitted Power upper threshold crossed*** alarm.

Cause

This alarm is raised when the transmitted power crosses above the upper threshold power for the SFP/XFP type which is used for the network element. This alarm will be cleared when the transmitted power is less than the specified upper threshold value.

Severity

Major

Object affected

Port

Impact

This alarm may affect traffic if the transmitted power level has crossed the upper threshold considerably.

Clearing procedure

1. This alarm indicates that SFP/XFP of the local network element is faulty. Replace the faulty SFP/XFP with an equivalent one.
2. Check if the **Transmitted Power upper threshold crossed** alarm is cleared at the local node.

If the alarm persists, contact your next level of support.

6 MS-SPRing/BLSR Alarms

This chapter describes MSSP alarms raised on Tejas Network Element and procedure to clear them. The alarm clearing procedures are based on MS-SPRing/BLSR protection.

6.1 Invalid K Byte - Trap ID:673

Use this procedure to clear the ***Invalid K Byte*** alarm.

Cause

This alarm is raised when one or more of the following conditions are present:

- Faulty fiber connection
- Mismatch between the given ring map and the actual ring topology

If east port of one is connected to east of other NE, similarly West port then Invalid k byte alarm is reported. Now issuing an exerciser command, the command is successfully accepted. The result of 'failure of exerciser' is shown in the events history page.

Severity

Major

Object affected

STM/OCn Port

Impact

The impact of the alarm is non-service affecting.

Clearing procedure

To clear this alarm, check the ring topology and ensure that they match the ring map provisioned on the network elements for the MS-SPRing/BLSR configuration.

If the alarm persists, contact your next level of support.

6.2 Invalid K Byte East - Trap ID:626

Use this procedure to clear the ***Invalid K Byte East*** alarm.

Cause

This alarm is raised when one or more of the following conditions are present:

- Faulty fiber connection.
- Mismatch between the given ring map and the actual ring topology.

Note: If East port of one is connected to east of other node, then Invalid k byte alarm is reported. Now issuing an exerciser command, the command successfully is accepted. The result of *failure* of *exerciser* is shown in the events history page.

Severity

Major

Object affected

MS-SPRing/BLSR

Impact

Traffic affecting

Clearing procedure

1. Check the ring topology and the fibre connections with the ring map.
2. Check if the ***Invalid K byte East*** alarm is cleared.

If the alarm persists, contact your next level of support.

6.3 Invalid K Byte West - Trap ID: 627

Use this procedure to clear the ***Invalid K Byte West*** alarm.

Cause

This alarm is raised when one or more of the following conditions are present:

- Faulty fiber connection
- Mismatch between the given ring map and the actual ring topology

Note: If West port of one is connected to west of other node, then Invalid k byte alarm is reported. Now issuing an exerciser command, the command successfully is accepted. The result of 'failure of exerciser' is shown in the events history page.

Severity

Major

Object affected

MS-SPRing/BLSR

Impact

Traffic affecting

Clearing procedure

1. Check the ring topology and the fibre connections with the ring map.

2. Check if the **Invalid K byte West** alarm is cleared.

If the alarm persists, contact your next level of support.

6.4 Manual Switch Active on East - Trap ID:632

Use this procedure to clear the ***Manual switch active on East*** alarm.

Cause

This alarm is raised on any STM/OCn ports belonging to an MSSPRing/BLSR group if Manual switch is applied on it.

Severity

Minor

Object affected

MS-SPRing/BLSR

Impact

Impact of this alarm is that the traffic will be switched to the STM/OCn port to which the manual switch is issued. The traffic will stay in the manually switched port or channel until again manually/forcefully switched away from this path or signal failure condition occurs on this path.

Clearing procedure

To clear the alarm,

1. Click **Protection** in the Navigation menu. Click **MSSP-Ring/BLSR** link. The MS-SPRing page is displayed.
2. Click on the desired MS-SPRing facility under the view field. The Protection Provisioning page is displayed.
3. Click **Clear** on the side (East) on which 'Manual Switch' was given (this can be found by seeing the alarm Ring switch, being present on east or west). A success message is displayed.
4. Check if the 'Manual switch active on East' alarm on STM/OC port is cleared. If the alarm is cleared, you have completed the procedure.

If the alarm persists, contact the next level of support.

6.5 Manual Switch Active On West - Trap ID:634

Use this procedure to clear the ***Manual switch active on West*** alarm.

Cause

This alarm is raised on any STM ports belonging to an MSSPRing/BLSR group if Manual switch is applied on it.

Severity

Minor

Object affected

MS-SPRing/BLSR

Impact

Impact of this alarm is that the traffic will be switched to the STM/OC port to which the manual switch is given. The traffic will stay in the manually switched port or channel until again manually/forcefully switched away from this path or signal failure condition occurs on this path.

Clearing procedure

To clear the alarm,

1. Click **Protection** in the Navigation menu. Click **MSSP-Ring** link. The MS-SPRing page is displayed.
2. Click on the desired MS-SPRing facility under the View field. The Protection Provisioning page is displayed.
3. Click **Clear** on the side (West) on which 'Manual Switch' was given (this can be found by seeing the alarm Ring switch, being present on east or west). A success message is displayed.
4. Check if the 'Manual switch active on West' alarm on STM/OC port is cleared. If the alarm is cleared, you have completed the procedure.

If the alarm persists, contact next level of support.

6.6 Ring Switch Active - Trap ID:672

Use this procedure to clear the ***Ring Switch Active*** alarm.

Cause

This alarm is raised when:

- External command like force or manual switch exists
- There is loss of signal, excessive errors or signal degrade on the optical port of the facility
- Card missing/ faulty card exists where the facility is provisioned
- Port admin is down at the location where the facility is provisioned

Any of the above cause is present in the adjacent node connected through that facility.

Severity

Major

Object affected

STM/OCn Port

Impact

The impact of the alarm is traffic affecting.

Clearing procedure

To clear the alarm,

1. Check for Forced switch active/Manual switch/signal fail/card missing or other active alarms present for the port/slot where the facility is provisioned.
2. Clear any active alarms by following respective trouble clearing procedures.

If the alarm persists, contact your next level of support.

6.7 Ring Switch East - Trap ID:423

Use this procedure to clear the ***Ring Switch East*** alarm.

Cause

This alarm is raised when:

- External command like force or manual switch exists
- There is loss of signal, excessive errors or signal degrade on the optical port of the facility
- Card missing/ faulty card exists where the facility is provisioned
- Port admin is down at the location where the facility is provisioned

Any of the above cause is present in the adjacent node connected through that facility.

Severity

Major

Object affected

MS-SPRing/BLSR

Impact

The impact of the alarm is traffic affecting.

Clearing procedure

To clear the alarm,

1. Check for Forced switch active/Manual switch/signal fail/card missing or other active alarms present for the port/slot where the facility is provisioned.
2. Clear any active alarms by following respective trouble clearing procedures.

If the alarm persists, contact your next level of support.

6.8 Ring Switch West - Trap ID:424

Use this procedure to clear the ***Ring Switch West*** alarm.

Cause

This alarm is raised when:

- External command like force or manual switch exists
- There is loss of signal, excessive errors or signal degrade on the optical port of the facility
- Card missing/ faulty card exists where the facility is provisioned
- Port admin is down at the location where the facility is provisioned

Any of the above cause is present in the adjacent node connected through that facility.

Severity

Major

Object Affected

MS-SPRing/BLSR

Impact

The impact of the alarm is traffic affecting.

Clearing Procedure

To clear the alarm,

1. Check for Forced switch active/Manual switch/signal fail/card missing or other active alarms present for the port/slot where the facility is provisioned.
2. Clear any active alarms by following respective trouble clearing procedures.

If the alarm persists, contact your next level of support.

This page is intentionally left blank

7 Security alarms

This chapter describes security based alarms raised on Tejas Network Elements and the procedures to clear these alarms.

7.1 All Radius Servers are Unavailable - Trap ID:647

Use this procedure to clear the ***All Radius Servers are Unavailable*** alarm.

Cause

This alarm is raised when the remote authentication request to all RADIUS servers expires after a user-provisionable timeout and no response is received from any RADIUS server.

Severity

Major

Object affected

Shelf

Impact

The impact of the alarm is non-service affecting.

Clearing procedure

To clear this alarm,

1. Verify RADIUS server is reachable from node. If not, provision at least one of the reachable RADIUS Server from UI and start the server.
2. If the alarm persists, check if one of the RADIUS server from UI has its secret key matching as that of the server. If the secret key is not the same, then edit the same.
3. Check if the "All Radius Servers are Unavailable" alarm is still present on local node.

If the alarm persists, contact your next level of support.

7.2 NE is Enrolled by the NMS/EMS - Trap ID:1206

Use this procedure to clear ***NE is Enrolled by the NMS/EMS*** alarm.

Cause

Node is enrolled by the NMS.

Severity

Minor

Object affected

System

Impact

The impact of the alarm is service affected.

Provisioning from node UI is disabled.

Clearing procedure

No action is required to clear this alarm. Alarm is cleared when the node is deleted from NMS.

If the alarm persists, contact your next level of support.

7.3 Primary Radius Server Unavailable - Trap ID:645

This procedure helps you clear the ***Primary Radius Server Unavailable*** alarm.

Cause

This alarm is raised when:

- remote authentication request to the Primary RADIUS server expires after a user-provisionable timeout and no response is received from the primary RADIUS server.
- DCN connectivity is lost between the network element and the RADIUS server.
- other parameters are incorrectly configured. For example, secret and vendor specific attributes.

Severity

Minor

Object affected

Radius

Impact

Non-traffic affecting. If no servers are reachable, the new management sessions (WUI, TL1) based on centralized user accounts may not be possible. User account changes on the RADIUS server may not be synchronized on the network element under this condition.

Clearing procedure

To clear this alarm,

1. Verify Primary RADIUS server is reachable from node. If not, provision a reachable Primary radius server and start the server.
2. If the alarm persists, check if the Primary RADIUS server from UI has its secret key matching as that of the server. If the secret key is not the same, then edit the same.

If the alarm persists, contact your next level of support.

7.4 Secondary Radius Servers Unavailable - Trap ID:646

Use this procedure to clear the ***Secondary Radius Server Unavailable*** alarm.

Cause

This alarm is raised when the remote authentication request to the secondary RADIUS server expires after a user-provisionable timeout and no response is received from the secondary RADIUS server.

Severity

Minor

Object affected

Radius

Impact

The impact of the alarm is non-service affecting.

Clearing procedure

To clear this alarm,

1. Verify Secondary RADIUS server is reachable from node. If not, provision a reachable Secondary radius server and start the server.
2. If alarm persists, check if the Secondary RADIUS server from UI has its secret key matching as that of the server. If the secret key is not the same, then edit the same.

If the alarm persists, contact your next level of support.

7.5 User Authentication Failed- Trap ID:320

Use this procedure to clear the ***User Authentication Failed*** alarm.

Cause

This alarm is raised when:

- an attempt to login into a TL1 session fails due to authentication.
- the user gives wrong credentials while logging in from web UI also.

This may be due to incorrect entry of user name and/or password. This alarm is raised when the user login is from TL1 interface.

Severity

Minor

Object affected

Node

Impact

The impact of the alarm is non-service affecting.

Clearing procedure

No action is required. This alarm is raised and automatically cleared by node after some time.

NOTE: User Name and Password are case sensitive. While typing the User Name or Password ensure that Caps Lock is disabled.

If the alarm persists, contact your next level of support.

7.6 User Password Expiry Warning – Trap ID: 1362

Use this procedure to clear the ***User Password Expiry Warning*** alarm.

Cause

This alarm is raised when the user password is about to expire.

Severity

Minor

Object affected

Tejusers

Impact

The impact of the alarm is non-service affecting.

Clearing procedure

To clear this alarm, change the user password.

If the alarm persists, contact your next level of support.

7.7 User Password Expired – Trap ID: 1363

Use this procedure to clear the ***User Password Expired*** alarm.

Cause

This alarm is raised when the user password is expired.

Severity

Major

Object affected

Tejusers

Impact

The impact of the alarm is non-service affecting.

Clearing procedure

To clear this alarm, change the user password.

If the alarm persists, contact your next level of support.

This page is intentionally left blank

8 OTN alarms

This chapter describes OTN alarms raised on Tejas Node and procedure to clear them.

8.1 Alarm Indication Signal on OTU Port - Trap ID:711

Use this procedure to clear ***Alarm Indication Signal on OTU Port*** alarm.

Cause

Alarm is raised when the incoming OTN signal does not have a valid payload. Alarm is typically raised as a consequent action to a LOS signal downstream.

Severity

Critical

Object affected

OTU Port

Impact

The impact of this alarm is that traffic through the respective port gets affected.

Clearing procedure

To clear this alarm,

1. Check the incoming OTU signal.
2. Determine next step.
   - If it is receiving Alarm indication signal, then go to step 3.
   - If it is not receiving Alarm indication signal contact your next level of support.
3. Check the far end node and determine next step.
   - If it is generating OTU Alarm Indication Signal without any other alarms on this node, then contact your next level of support.
   - If it is generating OTU Alarm Indication Signal with any other alarms on the node, then check for LOS, LOF, OTU-AIS alarms it is receiving which could have caused line AIS. Clear the alarms with appropriate alarm clearing procedure and go to step 4.

If the alarm persists, contact your next level of support.

8.2 Alarm Indication Signal - Trap ID:718

Use this procedure to clear ***Alarm Indication Signal*** alarm on ODU.

Cause

This is a downstream alarm raised to indicate defect in the upstream equipment in ODUk or in higher levels like OTUk.

Severity

Major

Object affected

ODU object

Impact

The impact of this alarm is that traffic through the respective port gets affected.

Clearing procedure

To clear this alarm,

1. Check the incoming ODU signal.
2. Determine next step from following:
   - If it is receiving Alarm indication signal, then go to step 3.
   - If it is not receiving Alarm indication signal contact your next level of support.
3. Check the far end node and determine next step from following:
   - If it is generating ODU Alarm Indication Signal without any other alarms on this node, then contact your next level of support.
   - If it is generating ODU Alarm Indication Signal with any other alarms on the node, then check for LOS, LOF, ODU-AIS, LOM, TIM, and DEG alarms it is receiving which could have caused line AIS. Clear the alarms with appropriate alarm clearing procedure and go to step 4.

If the alarm persists, contact your next level of support.

8.3 Alarm Indication Signal on ODU TCM - Trap ID:730

Use this procedure to clear ***Alarm Indication Signal*** alarm on ODU TCM.

Cause

This is a downstream alarm raised to indicate defect in upstream equipment in TCMn or higher layers.

Severity

Major

Object affected

ODU object

Impact

The impact of this alarm is that traffic through the respective port gets affected.

Clearing procedure

To clear this alarm,

1. Check the incoming ODU TCM signal.
2. Determine next step from the following:
   — If it is receiving Alarm indication signal, then go to step 3.
   — If it is not receiving Alarm indication signal contact your next level of support.
3. Check the far end node and determine next step from the following:
   — If it is generating ODU TCM Alarm Indication Signal without any other alarms on this node, then contact your next level of support.
   — If it is generating ODU TCM Alarm Indication Signal with any other alarms on the node, then check for TIM, DEG alarms it is receiving which could have caused TIM AIS. Clear the alarms with appropriate alarm clearing procedure.

If the alarm persists, contact your next level of support.

8.4 Backward Defect Indication - Trap ID:716

Use this procedure to clear ***Backward Defect Indication*** alarm on OTU port.

Cause

This is a remote alarm sent to Far-End node to indicate Near-End (NE) failures at OTUk levels like LOF, LOM, SD, TIM, etc.

Severity

Critical

Object affected

OTU port

Impact

The impact of this alarm is that traffic through the respective port gets affected.

Clearing procedure

1. If Backward defect indication alarm is raised on OTU, then Check for OTU-AIS, OTU-LOS and OTU-LOF alarms on far end node.
2. Determine next step from the following:
   — If the alarms are present on far end node, clear the alarms with appropriate alarm clearing procedure.
   — If the alarms are not present on far end node, contact your next level of support.

If the alarm persists contact your next level of support.

8.5 Backward Defect Indication - Trap ID:723

Use this procedure to clear ***Backward Defect Indication*** alarm on ODU object.

Cause

This is a remote alarm sent to Far-End node to indicate Near-end (NE) failures at ODUk level like LOFLOM, PLM, SD, TIM, OCI/LCK/AIS, etc.

Severity

Major

Object affected

ODU object

Impact

The impact of this alarm is that traffic through the respective path gets affected.

Clearing procedure

1. If Backward defect indication alarm is raised on ODU then check for OTU-AIS, OTU-LOS, OTU-LOF, LOM, TIM and DEG alarms on far end node.
2. Determine next step.
   — If the alarms are present on far end node, clear the alarms with appropriate alarm clearing procedure and go to step 3.
   — If the alarms are not present on far end node then contact your next level of support.

If the alarm persists contact your next level of support.

8.6 Backward Defect Indication on ODU TCM - Trap ID:760

Use this procedure to clear ***Backward Defect Indication*** alarm on ODU TCM object.

Cause

This is a remote alarm sent to Far-End node to indicate Near-End (NE) failures at TCMn level like OCI/LCK/AIS, TIM, etc.

Severity

Critical

Object affected

ODU TCM object

Impact

The impact of this alarm is that traffic through the respective path gets affected.

Clearing procedure

1. If Backward defect indication alarm is raised on ODU TCM then check for TIM, DEG alarms on far end node.
2. Determine next step from the following:

- If the alarms are present on far end node, clear the alarms with appropriate alarm clearing procedure and go to step 4.
- If the alarms are not present on far end node go to step 3.

3. Check for maintenance signals on far end if it is AIS/OCI/LCK and determine next step.
   - If the signals are present, change it to appropriate values.
   - If any of the above signals are not present then contact your next level of support.

If the alarm persists contact your next level of support.

8.7 Backward Incoming Alignment Error - Trap ID:713

Use this procedure to clear ***Backward Incoming Alignment Error*** alarm on OTU port.

Cause

This is a remote alarm sent to Far-End node to indicate IAE.

Severity

Major

Object affected

OTU port

Impact

The impact of this alarm is service affecting.

Clearing procedure

1. Check for OTU 'Incoming alignment error' alarm on far end node
2. Determine next step from the following:
   - If the alarm is present then clear the alarm with appropriate alarm clearing procedure.
   - If the alarm is not present then contact your next level of support.

If the alarm persists contact your next level of support.

8.8 Backward Incoming Alignment Error - Trap ID:761

Use this procedure to clear ***Backward Incoming Alignment Error*** alarm.

Cause

Alarm is raised when TCM is configured on the ODU connection. Alarm is raised on the ODU TCM object when the ODU object also has a backward incoming alignment error alarm.

Severity

Critical

Object affected

ODU TCM

Impact

No impact of this alarm. It only indicates a failure on the ODU connection which is tracked by a different alarm. Presence of this alarm on the ODU TCM object indicates that the TCM monitoring of this ODU cannot be done.

Clearing procedure

Clear the ODU level backward incoming alignment error alarm is cleared. Alarm will be cleared once the higher layer alarm clears.

If the alarm persists, contact your next level of support.

8.9 Bridged ODU - Trap ID:880

Use this procedure to clear ***Bridged ODU*** alarm on ODU.

Cause

This alarm is raised when the ODU is bridged on to a protecting ODU due to *Force switch* external command or *Signal fail* on work ODU.

Severity

Major

Object affected

ODU object

Impact

The impact of this alarm is service affecting.

Clearing procedure

1. Determine the step from the following:
   - If the 'Bridged ODU' alarm is raised due to 'Force switch' external command, then clear the 'Force switch' external command if it is the active request with appropriate alarm clearing procedure. The procedure is complete.
   - If the 'Bridged ODU' alarm is raised due to 'Signal fail' on work ODU, then go to step 2.
2. Check for the 'Signal fail' alarm on work ODU and protection group and determine next step from the following:
   - If the 'Signal fail' alarm is present and the protection group is provisioned as revertive, then clear the 'Signal fail' alarm with appropriate alarm clearing procedure.
   - If the 'Signal fail' alarm is present and the protection group is provisioned as non-revertive, then clear the 'Signal fail' alarm by applying 'Clear' external command.

If the alarm persists, contact your next level of support.

8.10 Client Signal Fail - Trap ID:793

Use this procedure to clear ***Client Signal*** alarm on ODU.

Cause

This alarm is raised due to client side LOS (Loss of Signal).

Severity

Major

Object affected

ODU object

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Trace the client interface which is mapped to the logical ODU, reporting this alarm and check for the alarm being reported on the client interface.
2. Alarm will clear automatically once the client side alarm is cleared.

If the alarm persists, contact your next level of support.

8.11 Client Defect - Trap ID:1126

Use this procedure to clear ***Client Defect*** alarm.

Cause

Alarm is specific to client interfaces like fiber channel and CPRI. Alarm is raised at the other end of a OTN connection when the incoming client signal is reporting a loss of optical power at the far end.

Severity

Critical

Object affected

OTN client port

Impact

Alarm indicates a client signal failure.

Clearing procedure

This alarm will automatically gets cleared once the fault on the client interface is cleared.

If the alarm persists, contact your next level of support.

8.12 Continuous APC regulation enabled - Trap ID: 1411

Use this procedure to clear **Continuous APC regulation enabled** alarm.

Cause

This alarm is raised when the **Continuous Regulation Enabled** parameter of the **ROADM** common port is set as **Enable.**

Severity

Critical

Object affected

Line port

Impact

The impact of this alarm is non-service affecting.

Clearing procedure

To clear this alarm, set the **Continuous Regulation Enabled** parameter of the **ROADM** common port as **Disable**.

If the alarm persists, contact your next level of support.

8.13 Degraded Defect on ODU - Trap ID: 722

Use this procedure to clear ***Degraded Defect*** alarm on ODU TCM.

Cause

This alarm is raised due to PM BIP errors crossing set threshold of DEGM/DEGTHRSH.

Severity

Major

Object affected

ODU TCM object

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check the OTU port for FEC uncorrectable errors on the interface, correct the same to clear this alarm

2. Alarm will get cleared automatically when the errors are reduced below the threshold which is set in the UI by the user.

If the alarm persists, contact your next level of support.

8.14 Degraded Defect on ODU TCM - Trap ID: 759

Use this procedure to clear ***Degraded Defect*** alarm on ODU.

Cause

This alarm is raised due to TCM BIP errors crossing set threshold of DEGM/DEGTHRSH.

Severity

Major

Object affected

ODU object

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check for OTU 'Signal degrade' alarm in the network, if you have a ODU connection. Determine next step.
   - If the alarm is present, then clear the alarm with appropriate alarm clearing procedure and go to step 4.
   - If the alarm is not present, then go to step 2.
2. Reroute the traffic through other port (probably through protected path using external commands if traffic is protected).
3. If the 'Degraded defect' alarm is raised on ODU, then check the cause for PM BIP8 error and rectify the error with appropriate procedure.
4. Check for the **Degraded defect** alarm.

If the alarm persists, contact your next level of support.

8.15 Extended Loss Of Frame - Trap ID: 724

Use this procedure to clear ***Extended Loss Of Frame*** alarm on ODU.

Cause

This alarm is raised to indicate loss of frame and multi-frame sequence in received ODU container (known as LOFLOM in the G.709 standard).

Severity

Major

Object affected

ODU object

Impact

The impact of this alarm is service affecting.

Clearing procedure

1. If *Extended loss of frame* alarm is present on ODU then corresponding ODU channel should be present on far end node, if not create same ODU channel on far end node.
2. Determine next step.
   - If the *Extended loss* of frame alarm clears, you have completed the procedure.
   - If the *Extended loss* of frame alarm persists, then go to step 3.
3. Check whether higher order ODU AIS is present on down the path or LOF present on far end. Determine next step.
   - If the higher order ODU AIS alarm is present, then clear the alarm with appropriate alarm clearing procedure. Go to step 5.
   - If the higher order ODU AIS alarm is not present, then go to step 4.
4. Check for any other alarms present on far end node and determine next step.
   - If the any alarms are present then clear the alarms with appropriate alarm clearing procedure. Go to step 4.
   - If the any alarms are not present, contact your next level of support.
5. Check if *Extended loss of frame* alarm is cleared at the local node.

If the alarm still persists, contact your next level of support.

8.16 Extended Loss Of MultiFrame - Trap ID: 725

Use this procedure to clear ***Extended Loss Of MultiFrame*** alarm on ODU.

Cause

Alarm indicates that the payload contained within an ODU multiframe is no longer available and is instead filled with an all 1s pattern. Alarm is raised due to a higher layer alarm on the OTU port or a fault in the connection trail.

Severity

Major

Object affected

ODU object

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. If alarm is present on ODU, then corresponding ODU channel should be present on far end node, if not create same ODU channel on far end node.
2. Check if the *Extended loss of multiframe* alarm is cleared and determine next step.
   — If the *Extended loss of multiframe* alarm clears, you have completed the procedure.
   — If the 'Extended loss of frame' alarm persists, then go to step 3.
3. Check for any other alarms present on far end node and determine next step.
   — If the alarms are present then clear the alarms with appropriate alarm clearing procedure. Go to step 4.
   — If the alarms are not present, then go to step 4.
4. Check if *Extended loss of frame* alarm is cleared at the local node.

If the alarm still persists, contact your next level of support.

8.17 Force Switch Active - Trap ID: 871

Use this procedure to clear ***Force Switch Active*** alarm on ODU.

NOTE: This alarm is applicable to OTU port if provisioned as part of a 1+1 MSP/APS.

Cause

This alarm is raised on OTU port when Force Switch is applied on ODU which should be a protect for some work ODU which is indicated by the additional trap argument.

Severity

Major

Object affected

OTU Port

Impact

The impact of this alarm is that the traffic protected by MSP will go in the path to which it is force switched to and will stay there even if it fails and the other path is in working condition.

Clearing procedure

To clear this alarm,

1. Click **Protection** in the Navigation menu of node UI. Then click on **ODU Path Linear Protection**. The **View ODU path linear protection** page is displayed.
2. Click on the link under the **View** field, against the desired protection group. The **ODUPathLinearProtectionGroup** page is displayed.
3. Click ***Clear*** under **External Commands** field. The Connections protection request confirm page is displayed.
4. Click **Confirm request**. The Connections protection request result page is displayed with a success message.

5. Check if the 'Forced Switch Active' alarm on ODU is cleared at the local node.

If the alarm persists, contact your next level of support.

8.18 Force Switch Extra Traffic Signal Active - Trap ID:876

Use this procedure to clear ***Force Switch Extra Traffic Signal Active*** alarm on ODU.

NOTE: This alarm is applicable to OTU port if provisioned as part of a 1+1 MSP/APS.

Cause

This alarm is raised when Force switch extra traffic signal is applied on ODU which should be a protecting entity.

Severity

Major

Object affected

OTU Port

Impact

The impact of this alarm is that the traffic protected by MSP will go in the path to which it is force switched to and will stay there even if it fails and the other path is in working condition.

Clearing procedure

To clear this alarm, apply the clear command from the node UI.

If the alarm persists, contact your next level of support.

8.19 Force Switch Null Signal Active - Trap ID:875

Use this procedure to clear ***Force Switch Null Signal Active*** alarm on ODU.

NOTE: This alarm is applicable to OTU port if provisioned as part of a 1+1 MSP/APS.

Cause

This alarm is raised when Force switch null signal active is applied on ODU which should be a protecting entity.

Severity

Major

Object affected

OTU Port

Impact

The impact of this alarm is that the traffic protected by MSP will go in the path to which it is force switched to and will stay there even if it fails and the other path is in working condition.

Clearing procedure

To clear this alarm, apply the clear command from the node UI.

If the alarm persists, contact your next level of support.

8.20 Incoming Alignment Error - Trap ID:712

Use this procedure to clear ***Incoming Alignment Error*** alarm on OTU port.

Cause

This is a downstream alarm to indicate frame slip event reported in upstream equipment.

Severity

Major

Object affected

OTU Port

Impact

The impact of this alarm is service affecting.

Clearing procedure

1. Check for *OOF* alarm on upstream side on far end node and determine next step from the following:
   - If the alarm is present, then clear the alarm with appropriate alarm clearing procedure and go to step 2.
   - If the OOF alarm is not present, then contact your next level of support.
2. Check if the *Incoming alignment error* alarm is cleared.

If the alarm persists, contact your next level of support.

8.21 Incoming Alignment Error on ODU TCM - Trap ID:758

Use this procedure to clear ***Incoming Alignment Error*** alarm.

Cause

Alarm is raised only when TCM is configured on the ODU connection. Alarm is raised on the ODU TCM object when the ODU object also has a incoming alignment error alarm.

Severity

Major

Object affected

ODU TCM

Impact

No impact of this alarm. It only indicates a failure on the ODU connection which is tracked by a different alarm. Presence of this alarm on the ODU TCM object indicates that the TCM monitoring of this ODU cannot be done.

Clearing procedure

To clear this alarm, clear the ODU level incoming alignment error. Alarm will be cleared once the higher layer alarm clears.

If the alarm persists, contact your next level of support.

8.22 Laser is shutdown Due to RPP - Trap ID:1334

Use this procedure to clear ***Laser is shutdown Due to RPP*** alarm.

Cause

The laser shuts down when the RPP feature is enabled on the transponder and the paired port has LOS.

Severity

Major

Object affected

Port

Impact

The impact of the alarm is service affective.

Clearing procedure

To clear the alarm, clear LOS alarm on the paired port or disable RPP.

8.23 Local fault - Trap ID: 1403

Use this procedure to clear ***Local fault*** alarm.

Cause

This alarm is raised when there is a signal loss, synchronization loss, and high bit error rate due to the link down or link failure issues.

Severity

Critical

Object affected

Ethernet port

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm, check the physical connectivity and correct it. The alarm clears when proper connection is made.

If the alarm still persists, contact your next level of support.

8.24 Lockout Active - Trap ID:877

Use this procedure to clear ***Lockout Active*** alarm.

Cause

Alarm indicates a user initiated lockout of protection triggered from the node UI on the ODU connection.

Severity

Major

Object affected

ODU

Impact

The impact of the alarm affects protection switching. Any alarm raised on the work path when lockout is active causes the traffic to go down.

Clearing procedure

To clear this alarm, apply clear command from the node UI.

If the alarm still persists, contact your next level of support.

8.25 Loss of Block Synchronization - Trap ID:1270

Use this procedure to clear ***loss of block synchronization*** alarm.

Cause

Alarm is specific to client interfaces like fiber channel and CPRI. Alarm is raised when the incoming client signal is reporting a loss of framing sequence. The alarm is typically due to low input optical power, or a high level of errors on that interface. The framing sequence can be lost if a wrong client signal is connected to the port.

Severity

Critical

Object affected

OTN client port

Impact

Alarm indicates a client signal failure.

Clearing procedure

To clear this alarm,

1. Check for the fiber path to correct the cause of low input power at the client interface.
2. Check the connected device to the client interface and ensure that the port on the connected device is as per the client port which is connected on our system.

If the alarm persists, contact your next level of support.

8.26 Locked Defect - Trap ID:719

Use this procedure to clear ***Locked Defect*** alarm.

Cause

This alarm is used during maintenance operation in a network segment. The LCK defect is sent towards either side of the segment to prevent test data from entering the client network.

Severity

Major

Object affected

OTU Port

Impact

The impact of this alarm is service affecting.

Clearing procedure

1. Check the ODU channel present on far end node is sending LCK test signal and determine next step from the following.
   — If it is sending LCK test signal, then change it to appropriate value and go to step 2.
   — If it is not sending LCK test signal, contact your next level of support.
2. Check for the *Locked defect* alarm.

If the alarm persists, contact your next level of support.

8.27 Locked Defect on ODU TCM - Trap ID:731

Use this procedure to clear ***Locked Defect*** alarm.

Cause

Alarm is raised only when TCM is configured on the ODU connection. Alarm is raised on the ODU TCM object when the ODU object also has a LCK alarm.

Severity

Major

Object affected

ODU TCM

Impact

No impact of this alarm, it indicates a failure on the ODU connection which is tracked by a different alarm. Presence of this alarm on the ODU TCM object indicates that the TCM monitoring of this ODU cannot be done.

Clearing procedure

Alarm will clear once the ODU level LCK alarm is cleared. Alarm will clear automatically once the higher layer alarm clears.

If the alarm persists, contact your next level of support.

8.28 Loss of Frame - Trap ID:709

Use this procedure to clear ***Loss of Frame*** alarm on OTU port.

Cause

This alarm is raised due to upstream equipment/card failure or due to upstream fiber cut in DWDM link with amplifier.

Severity

Critical

Object affected

OTU Port

Impact

The impact of this alarm on OTU is traffic affecting.

Clearing procedure

To clear this alarm,

1. Identify the OTU port raising the alarm.
2. Clean the receive optical connections at the near end node. Use the appropriate company procedure to clean the optical fibers and connectors. Check the received optical power is within the correct range.
3. Determine next step from the following:
   — If the optical power is in the correct range, then go to step 6.
   — If the optical power is not in the correct range, then go to step 4.
4. Clean the transmit optical connections at the far end node. Use the appropriate company procedure to clean the optical fibers and connectors. Check that transmit optical power is within correct range.
5. Determine next step from the following:
   — If the transmit optical power is in the correct range the fault is associated with the optical fiber. Use appropriate methods to isolate fiber fault. Go to step 6.
   — If the transmit optical power is not in the correct range, then contact your next level of support.
6. Check for the *Loss of Frame* alarm.

If the alarm persists, then contact your next level of support.

8.29 Loss of Frame - Trap ID:1269

Use this procedure to clear ***Loss of Frame*** alarm.

Cause

Alarm is specific to client interfaces like fiber channel and CPRI. Alarm is raised when the incoming client signal is reporting a loss of framing sequence. The alarm is due to low input optical power or a high level of errors on that interface. The framing sequence can be lost if a wrong client signal is connected to the port.

Severity

Critical

Object affected

OTN client port

Impact

Alarm indicates a client signal failure.

Clearing procedure

To clear this alarm,

1. Check for the fiber path to correct the cause of low input power at the client interface.

2. Check the connected device to the client interface and ensure that the port on the connected device is as per the client port which is connected on our system.

If the alarm persists, contact your next level of support.

8.30 Loss of MultiFrame - Trap ID:710

Use this procedure to clear ***Loss of MultiFrame*** alarm on OTU port.

Cause

This alarm is raised due to upstream equipment/card failure or due to mismatched FEC type/enable configuration.

Severity

Critical

Object affected

OTU Port

Impact

The impact of this alarm are:

- traffic affecting on unprotected paths.
- temporary traffic hit on the protected paths, if the paths switched to aggregate containing no alarm.

Clearing procedure

To clear this alarm,

1. Identify the OTU port raising the alarm.
2. Clean the receive optical connections at the near end node. Use the appropriate company procedure to clean the optical fibers and connectors. Check the received optical power is within the correct range.
3. Determine next step.
   — If the optical power is in the correct range, then go to step 6.
   — If the optical power is not in the correct range, then go to step 4.
4. Clean the transmit optical connections at the far end node. Use the appropriate company procedure to clean the optical fibers and connectors. Check that transmit optical power is within correct range.
5. Determine next step.
   — If the transmit optical power is in the correct range the fault is associated with the optical fiber. Use appropriate methods to isolate fiber fault. Go to step 6.
   — If the transmit optical power is not in the correct range, then contact your next level of support.
6. Check for the *Loss of MultiFrame* alarm.

If the alarm persists, then contact your next level of support.

8.31 Loss of Signal - Trap ID:706

Use this procedure to clear ***Loss of Signal*** alarm on OTU port.

Cause

This alarm is raised on STM/OCN ports and OTU ports, when:

- received signal level drops below an implementation determined threshold. This may be due to:
  - port admin down at far end
  - fiber cuts
  - faulty fibers
  - dusty fibers
  - faulty receiver
- SFP/XFP not inserted properly in the SFP/XFP cage.

Severity

Critical

Object affected

OTU Port

Impact

The impact of this alarm are:

- Traffic affecting on unprotected paths.
- operational status of the associated unprotected cross connections down.
- traffic on the respective interface in error.
- temporary traffic hit if path switched to protecting one in case of
- Protected cross connections or MSP/APS protection scheme.
- Management connectivity will be lost on that interface.
- Loss of synchronization if node locked to that port and the remaining clock switching depends on the nomination of other clock.

Clearing procedure

To clear this alarm,

1. Identify the OTU port raising the alarm.
2. Clean the receive optical connections at the near end node. Use the appropriate company procedure to clean the optical fibers and connectors. Check the received optical power is within the correct range.
3. Determine next step.
   - If the optical power is in the correct range, then go to step 6.
   - If the optical power is not in the correct range, then go to step 4.

4. Clean the transmit optical connections at the far end node. Use the appropriate company procedure to clean the optical fibers and connectors. Check that transmit optical power is within correct range.
5. Determine next step.
   - If the transmit optical power is in the correct range the fault is associated with the optical fiber. Use appropriate methods to isolate fiber fault. Go to step 6.
   - If the transmit optical power is not in the correct range, then contact your next level of support.
6. Check for the *Loss of Signal* alarm.

If the alarm persists, then contact your next level of support.

8.32 Loss of Signal - Trap ID:1125

Use this procedure to clear ***Loss of Signal*** alarm.

Cause

Alarm is specific to client interfaces like fiber channel and CPRI. Alarm is raised when the incoming client signal is reporting a loss of optical power and when the client optics detect the loss of the optical signal.

Severity

Critical

Object affected

OTN client port

Impact

Alarm indicates a client signal failure.

Clearing procedure

To clear this alarm, check for the fiber path to correct the cause of low input power at the client interface.

If the alarm persists, contact your next level of support.

8.33 Loss of Tandem Connection - Trap ID:762

Use this procedure to clear ***Loss of Tandem Connection*** alarm on ODU TCM.

Cause

This alarm is raised due to TCM channel failure or due to de-provisioning in upstream equipment.

Severity

Major

Object affected

ODU TCM

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Verify if TCMn is enabled on corresponding ODU channel on far end node.
   — If TCMn is enabled, then contact your next level of support.
   — If TCMn is not enabled, then enable it and Go to step 2.
2. Check if the *Loss of Tandem Connection* alarm is cleared on local node.

If the alarm persists, contact your next level of support.

8.34 Manual Switch Active - Trap ID:872

Use this procedure to clear '*Manual Switch Active*' alarm on ODU.

NOTE: This alarm is applicable to OTU port if provisioned as part of a 1+1 MSP/APS.

Cause

This alarm is raised on ODU when Manual Switch is applied on ODU which should be a protect for some work ODU.

Severity

Major

Object affected

ODU

Impact

Impact of this alarm is that the traffic will be switched to the ODU channel to which the manual switch is given. The traffic will stay in the manually switched port until again manually/forcefully switched away from this path or signal failure condition occurs on this path.

Clearing procedure

To clear this alarm,

1. Click **Protection** in the Navigation menu of node UI. Then click on **ODU Path Linear Protection**. The **View ODU path linear protection** page is displayed.
2. Click on the link under the **View** field, against the desired protection group. The **ODUPathLinearProtectionGroup** page is displayed.
3. Click ***Clear*** under **External Commands** field. The Connections protection request confirm page is displayed.

4. Click ***Confirm request***. The Connections protection request result page is displayed with a success message.
5. Check if the 'Manual Switch Active' alarm on ODU is cleared at the local node.

If the alarm persists, contact your next level of support.

8.35 Manual Switch Null Signal Active - Trap ID:873

Use this procedure to clear ***Manual Switch Null Signal Active*** alarm on ODU.

NOTE: This alarm is applicable to OTU port if provisioned as part of a 1+1 MSP/APS.

Cause

This alarm is raised on ODU when Manual Switch is applied on ODU which should be a protect for some work ODU.

Severity

Major

Object affected

ODU

Impact

Impact of this alarm is that the traffic will be switched to the ODU channel to which the manual switch is given. The traffic will stay in the manually switched port until again manually/forcefully switched away from this path or signal failure condition occurs on this path.

Clearing procedure

To clear this alarm, apply the clear command from the node node UI.

If the alarm persists, contact your next level of support.

8.36 MultiPlex Structure Identifier Mismatch - Trap ID:728

Use this procedure to clear ***MultiPlex Structure Identifier Mismatch*** alarm on ODU.

Cause

This alarm is raised due to mismatch in the incoming multiplexing structure with respect to the expected one or due to wrong configurations of ODUj channels.

Severity

Major

Object affected

OTU Port

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check the corresponding far end node for corresponding ODU transmit MultiPlex Structure Identifier Mismatch value. If transmitted value on far end node is not same as expected on near end node then change it to appropriate value. Check if the 'Multiplex Structure Identifier Mismatch' alarm is cleared.
   — If the 'MultiPlex Structure Identifier Mismatch' alarm clears, then you have completed the procedure.
   — If the 'MultiPlex Structure Identifier Mismatch' alarm persists, go to step 2.
2. Check if far end node has ODU connection, trace the node where there is no ODU connection on the corresponding ODU channel and change the MultiPlex Structure Identifier Mismatch value to some other appropriate value. Check if the 'Multiplex Structure Identifier Mismatch' alarm is cleared on local node.
   — If the 'MultiPlex Structure Identifier Mismatch' alarm clears, then you have completed the procedure.

If the alarm persists, then contact your next level of support.

8.37 NULL Test Signal - Trap ID:922

Use this procedure to clear ***NULL Test Signal*** alarm on ODU.

Cause

This alarm is caused due to test signal used during commissioning or maintenance testing where signal payload comprises of all 0's.

Severity

Minor

Object affected

OTU Port

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check the ODU channel present on far end node is sending Null test signal.
   — If it is sending null test signal, then change it to appropriate value and go to step 2.
   — If it is not sending null test signal, then contact your next level of support.

2. Check if the *NULL Test Signal* alarm is cleared on local node.

If the alarm persists, then contact your next level of support.

8.38 ODULinearProtection APS bit Mismatch - Trap ID:1123

Use this procedure to clear ***ODULinearProtection APS bit Mismatch*** alarm.

Cause

This alarm is raised when the 'A' bit of the transmitted and accepted APS protocol do not match.

Severity

Major

Object affected

ODU Path Linear Protection Group

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Provision both the inter-networking protection groups with same A bit (Protection Switching through APS bytes/without APS Bytes) of MSP/APS Protocol. Check for the *ODULinearProtection APS bit Mismatch* alarm.
   — If the alarm is clears, you have completed the procedure.

If the alarm persists, contact your next level of support.

8.39 ODULinearProtection Bridged Signal Mismatch - Trap ID:882

Use this procedure to clear ***ODULinearProtection Bridged Signal Mismatch*** alarm.

Cause

This alarm is raised when the requested signal and the incoming bridge signal in the MSP/APS protocol do not match within 1 second.

Severity

Major

Object affected

ODU

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Provision both the internetworking protection groups with same B bit (1+1/1:1) of MSP/APS protocol.
   - If the *ODULinearProtection Bridged Signal Mismatch* alarm clears, then you have completed the procedure.
   - If the *ODULinearProtection Bridged Signal Mismatch* alarm persists, then go to step 2.
2. Check if there is any *Signal fail* alarm on protected ODU.
   - If the Signal Fail alarm is present, then clear the alarm with appropriate alarm clearing procedure. Go to step 3.
   - If the Signal Fail alarm is not present, then contact your next level of support.
3. Check if the *ODULinearProtection Bridged Signal Mismatch* alarm is cleared on local node.

If the alarm persists, then contact your next level of support.

8.40 ODULinearProtection Direction Mismatch - Trap ID:1124

Use this procedure to clear ***ODULinearProtection Direction Mismatch*** alarm.

Cause

This alarm is raised when the D bit of the transmitted and accepted MSP/APS protocol do not match.

Severity

Major

Object affected

ODU Path Linear Protection Group

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm, provision both the internetworking protection groups with same D bit (unidirectional switching/bidirectional switching) of MSP/APS protocol.

- If the 'ODULinearProtection Direction Mismatch' alarm clears, then you have completed the procedure.

If the alarm persists, then contact your next level of support.

8.41 ODULinearProtection Freeze Active - Trap ID:884

Use this procedure to clear ***ODULinearProtection Freeze Active*** alarm.

Cause

This alarm is raised when *Freeze* external command is applied.

Severity

Major

Object affected

ODU Path Linear Protection Group

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Click **Protection** in the Navigation menu of node UI. Then click on **ODU Path Linear Protection**. The **View ODU path linear protection** page is displayed.
2. Click on the link under the **View** field, against the desired protection group. The **ODUPathLinearProtectionGroup** page is displayed.
3. Click **Clear Freeze** under **External Commands** field. The Connections protection request confirm page is displayed.
4. Click **Confirm request**. The Connections protection request result page is displayed with a success message.
5. Check if the *ODULinearProtection Freeze Active* alarm is cleared at the local node.

If the alarm persists, contact your next level of support.

8.42 ODULinearProtection Manual Switch Extra Traffic Signal Active - Trap ID:874

Use this procedure to clear ***ODULinearProtection Manual Switch Extra Traffic Signal Active*** alarm on ODU.

NOTE: This alarm is applicable to OTU port if provisioned as part of a 1+1 MSP/APS.

Cause

This alarm is raised when manual switch extra traffic signal is applied on this ODU which should be a protecting entity.

Severity

Major

Object affected

ODU

Impact

Impact of this alarm is traffic affecting.

Clearing procedure

To clear this alarm, apply the clear command from the node node UI.

If the alarm persists, contact your next level of support.

8.43 ODULinearProtection Provision Mismatch - Trap ID:883

Use this procedure to clear ***ODULinearProtection Provision Mismatch*** alarm.

Cause

This alarm is raised when the B bit of the transmitted and accepted APS protocol do not match.

Severity

Major

Object affected

ODUPathLinearProtectionGroup

Impact

The impact of this alarm is service affecting.

Clearing procedure

Provision both the internetworking protection groups with same B bit (1+1/1:1) of MSP/ APS protocol. Check if the *ODULinearProtection Provision Mismatch* alarm on ODU is cleared at the local node.

If the alarm persists, then contact your next level of support.

8.44 Open Connection Indication - Trap ID:717

Use this procedure to clear ***Open Connection Indication*** alarm.

Cause

This alarm is caused due to absence of ODU cross-connect provisioning in upstream direction.

Severity

Critical

Object affected

ODU

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check the ODU connection on corresponding ODU channel on far end node exists. If it does not exists, create the connection. Check for the 'Open Connection Indication' alarm.
   - If the alarm clears, then you have completed the procedure.
   - If the alarm persists, then go to step 2.
2. Check for any mismatch of ODU connection configuration between local node and far end node, for example ODU0 in one node and ODU1 in other node.
   - If there is mismatch, then correct it with appropriate procedure. Go to step 4.
   - If there is no mismatch, then go to step 3.
3. Check for maintenance and test signal attribute of ODU channel. It should not be ODU Open connection indication alarm if ODU connection exists.
4. Check for the 'Open Connection Indication' alarm.
   - If the alarm clears, then you have completed the procedure.

If the alarm persists, contact your next level of support.

8.45 Open Connection Indication on ODU TCM - Trap ID:729

Use this procedure to clear ***Open Connection Indication*** alarm.

Cause

This alarm is raised when TCM is configured on the ODU connection and the other end does not have a corresponding connecting object/TCM object.

Severity

Critical

Object affected

ODU TCM

Impact

No impact of this alarm. It only indicates a failure on the ODU connection which is tracked by a different alarm. Presence of this alarm on the ODU TCM object indicates that the TCM monitoring of this ODU cannot be done.

Clearing procedure

To clear this alarm, trace the connection and check that the ODU TCM is enabled on the connection. Alarm will be cleared once the missing ODU TCM is recreated.

If the alarm persists, contact your next level of support.

8.46 PayLoad Mismatch - Trap ID:726

Use this procedure to clear ***PayLoad Mismatch*** alarm.

Cause

This alarm is raised due to wrong configuration of expected payload type in node or due to wrong transmitted payload type in upstream.

Severity

Major

Object affected

ODU

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check the corresponding far end node for corresponding ODU transmit payload type.
   - If it is an experimental mapping, then change it to some appropriate value.
   - If it is not an experimental mapping, then go to step 2.
2. Check if far end node has ODU connection, trace the node where there is no ODU connection on the corresponding ODU channel and change the transmit payload type to some other appropriate value. Check if the 'Payload Mismatch' alarm is cleared on local node.
   - If the alarm clears, then you have completed the procedure.

If the alarm persists, then contact your next level of support.

8.47 PRBS Test Signal - Trap ID:921

Use this procedure to clear ***PRBS Test Signal*** alarm on ODU.

Cause

This alarm is raised due to test signal used during commissioning or maintenance testing where signal payload comprises of PRBS31 pattern.

Severity

Minor

Object affected

OTU Port

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check the ODU channel present on far end node is sending PRBS test signal.
   - — If it is sending PRBS test signal, then change it to appropriate value and go to step 2.
   - — If it is not sending PRBS test signal, then contact your next level of support.
2. Check if the *PRBS Test Signal* alarm is cleared on local node.

If the alarm persists, then contact your next level of support.

8.48 Pre FEC Signal Degrade - Trap ID:1256

Use this procedure to clear ***Pre FEC Signal Degrade*** alarm.

Cause

Alarm is raised against the OTU port indicating errors beyond a particular rate which are getting corrected due to FEC on the OTN port. This degrade threshold is different from the threshold at which the degraded defect alarm is raised.

Severity

Major

Object affected

OTU port

Impact

- If the connection is protected then a protection switch is triggered and traffic switches to the protect path.

- If the ODU is unprotected then alarm is raised, but no impact on the actual traffic since FEC will correct the errors automatically.

Clearing procedure

To clear this alarm, check for the fiber path to correct the cause of incoming errors at the client interface.

If the alarm persists, contact your next level of support.

8.49 Remote fault - Trap ID: 1404

Use this procedure to clear ***Remote fault*** alarm.

Cause

This alarm is raised on a node when a **local fault** alarm is raised on a remote node.

Severity

Critical

Object affected

Ethernet port

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm, check the physical connectivity of the link causing local fault on the remote node and correct it. The alarm clears when proper connection is made.

If the alarm still persists, contact your next level of support.

8.50 Selected ODU - Trap ID:881

Use this procedure to clear ***Selected ODU*** alarm.

Cause

This alarm is raised when a protected ODU is selected from a protecting ODU due to:

- Force switch external command or
- Signal fail on work ODU.

Severity

Major

Object affected

ODU

Impact

The impact of this alarm is service affecting.

Clearing procedure

1. Determine the step.
   - If the *Selected ODU* alarm is raised due to 'Force switch' external command, then clear the 'Force switch' external command if it is the active request with appropriate alarm clearing procedure. Go to step 3.
   - If the *Selected ODU* alarm is raised due to 'Signal fail' on work ODU, then go to step 2.
2. Check for the 'Signal fail' alarm on work ODU and protection group.
   - If the 'Signal fail' alarm is present and the protection group is provisioned as revertive, then clear the 'Signal fail' alarm with appropriate alarm clearing procedure. Go to step 3.
   - If the 'Signal fail' alarm is present and the protection group is provisioned as non revertive, then clear the 'Signal fail' alarm by applying 'Clear' external command. Go to step 3.
3. Check if the *Selected ODU* alarm is cleared on local node.

If the alarm persists contact your next level of support.

8.51 Signal Fail - Trap ID:1128

Use this procedure to clear ***Signal Fail*** alarm.

Cause

Alarm is specific to client interfaces like fiber channel and CPRI. Alarm is raised when the incoming client signal is reporting errors in the signal. The error rate is above a set threshold for reporting the signal fail alarm.

Severity

Critical

Object affected

OTN client port

Impact

Alarm indicates an incoming error signal. These errors will be transparently carried over the OTN connection.

Clearing procedure

To clear this alarm, check for the fiber path to correct the cause of incoming errors at the client interface.

If the alarm persists, contact your next level of support.

8.52 Server Signal Degrade on ODU - Trap ID:721

Use this procedure to clear ***Server Signal Degrade*** alarm on ODU.

Cause

Alarm indicates error in the higher layer resulting error in the lower layer. In this case OTU port associated with ODU object will report an error link.

Severity

Major

Object affected

ODU

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check for lower order alarms on channelized ODU or TCM. Clear the alarms with appropriate alarm clearing procedure.
2. Check if the 'Server Signal Degrade' alarm is cleared on local node.

If the alarm persists, contact your next level of support.

8.53 Server Signal Degrade on ODU TCM - Trap ID:705

Use this procedure to clear ***Server Signal Degrade*** alarm on ODU TCM.

Cause

Alarm is raised when TCM is configured on the ODU connection and when the associated ODU object has a server signal degrade alarm.

Severity

Major

Object affected

ODU TCM

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check for any other alarms present on channelized ODU or TCM. Clear the alarms with appropriate alarm clearing procedure.
2. Check if the *Server Signal Degrade* alarm is cleared on local node.

If the alarm persists, contact your next level of support.

8.54 Signal Degrade - Trap ID:714

Use this procedure to clear ***Signal Degrade*** alarm.

Cause

This alarm is raised when an incoming OTN signal has errors which is beyond a threshold value.

Severity

Major

Object affected

OTU port

Impact

In case of protected link, protection switch is triggered and traffic switches to protected path. In case of unprotected link, traffic is affected till fault condition is cleared.

Clearing procedure

Check the fiber path to see where the errors are being reported and correct the same. Alarm will clear automatically once the error condition is removed.

If the alarm persists, contact your next level of support.

8.55 Signal Degrade - Trap ID:1127

Use this procedure to clear ***Signal Degrade*** alarm.

Cause

Alarm is specific to client interfaces like fiber channel and CPRI. Alarm is raised when the incoming client signal is reporting errors in the signal. The error rate is above a set threshold for reporting the degrade alarm.

Severity

Major

Object affected

OTN client port

Impact

Alarm indicates an incoming error signal. These errors will be transparently carried over the OTN connection.

Clearing procedure

To clear this alarm, check for the fiber path to correct the cause of incoming errors at the client interface for the fiber path to correct the cause of incoming errors at the client interface.

If the alarm persists, contact your next level of support.

8.56 Server Signal Fail- Trap ID:727

Use this procedure to clear ***Server Signal Fail*** alarm.

Cause

Alarm indicating a defect in the higher layer results a defect in lower layer. In this case OTU port associated with ODU objects reports a defect.

Severity

Major

Object affected

ODU

Impact

The impact of the alarm is traffic affecting for unprotected traffic.

Clearing procedure

Clearance of the higher layer alarm on the OTU port associated with the ODU object would result in the automatic clearance of this alarm.

If the alarm persists, contact your next level of support.

8.57 Server Signal Fail on ODU TCM - Trap ID:770

Use this procedure to clear ***Server Signal Fail*** alarm.

Cause

Alarm is raised when TCM is configured on the ODU connection and when the associated ODU object also has a server signal fail alarm.

Severity

Major

Object affected

ODU TCM

Impact

No impact of this alarm. It indicates a failure on the ODU connection which is tracked by a different alarm. Presence of this alarm on the ODU TCM object indicates that the TCM monitoring of this ODU cannot be done.

Clearing procedure

To clear this alarm, clear the ODU level server signal fail alarm. Alarm will be cleared once the higher layer alarm clears.

If the alarm persists, contact your next level of support.

8.58 Trail Trace Identifier Mismatch - Trap ID:715

Use this procedure to clear ***Trail Trace Identifier Mismatch*** alarm.

Cause

Alarm indicates that there is a mismatch in the SAPI/DAPI from what is expected by the interface. Alarm is raised when there is a misconnection in the fiber which causes different SAPI/DAPI to be recieved than what is expected.

Severity

Major

Object affected

OTU port

Impact

Impact of this alarm depends on the configuration of the action for TTI Mismatch.

- Downstream AIS configured on TTI Mismatch causes an OTU AIS to send downstream on receipt of this alarm.
- Alarm can be reported without sending downstream AIS alarm.

Clearing procedure

To clear this alarm,

1. Detect the misconnection of the fiber and correct the same.
2. If the change in fiber is intentional then correct the expected SAPI/DAPI to reflect the new values as per the new fiber connection.

If the alarm persists, contact your next level of support.

8.59 Trail Trace Identifier Mismatch on ODU - Trap ID: 720

Use this procedure to clear ***Trial Trace Identifier Mismatch*** alarm.

Cause

Alarm indicating that there is a mismatch in the SAPI/DAPI from what is expected by the interface. Alarm is raised when there is a misconnection in the fiber which causes different SAPI/DAPI to be received than what is expected.

Severity

Major

Object affected

ODU

Impact

Impact of this alarm depends on the configuration of the action for TTI Mismatch.

- Downstream AIS configured on TTI Mismatch causes an OTU AIS to send downstream on receipt of this alarm.
- Alarm can be reported without sending downstream AIS alarm.

Clearing procedure

To clear this alarm,

1. Detect the misconnection of the fiber and correct the same.
2. If the change in fiber is intentional then correct the expected SAPI/DAPI to reflect the new values as per the new fiber connection.

If the alarm persists, contact your next level of support.

8.60 Trail Trace Identifier Mismatch on ODU TCM - Trap ID:757

Use this procedure to clear ***Trail Trace Identifier Mismatch*** alarms.

Cause

Alarm is raised when TCM is configured on the ODU connection and the associated ODU object also has a TTI mismatch alarm.

Severity

Major

Object affected

ODU TCM

Impact

No impact of this alarm. It only indicates a failure on the ODU connection which is tracked by a different alarm. Presence of this alarm on the ODU TCM object indicates that the TCM monitoring of this ODU cannot be done.

Clearing procedure

Clear the ODU level TTI alarm. Alarm will be cleared once the higher layer alarm clears.

If the alarm persists, contact your next level of support.

This page is intentionally left blank

9 DWDM alarms

This chapter describes DWDM alarms raised and procedure to clear them.

9.1 Amplifier Pump Over Current - Trap ID:1073

Use this procedure to clear ***Amplifier pump over current*** alarm.

Cause

The alarm is raised when pump current value goes beyond the threshold. The current value goes beyond the threshold due to aging, and temperature variant. The pump current of the Amplifier port can be monitored under **Performance** menu for Current interval, 15min Intervals and Previous Day.

Severity

Critical

Object affected

Optical Amplifier Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

Check the path as well as the far end node for **Input Power (dBm)**. Ensure that the power received from far end on the Amplifier Port is within the limits.

If the alarm persists, contact your next level of support.

9.2 Amplifier Pump High Temperature - Trap ID:1074

Use this procedure to clear ***Amplifier pump high temperature*** alarm.

Cause

The alarm is raised when pump temperature goes beyond the threshold. The pump temperature of the Amplifier port can be monitored under **Performance** menu for Current interval, 15min Intervals and Previous Day.

Severity

Critical

Object affected

Optical Amplifier Port

Impact

The impact of the alarm is traffic affecting if it exists for long duration.

Clearing procedure

Amplifier pump high temperature alarm will get cleared when temperature is set within the operating range.

If the alarm persists, contact your next level of support.

9.3 Amplifier Case Low Temperature - Trap ID: 1075

Use this procedure to clear ***Amplifier case low temperature*** alarm.

Cause

This alarm is raised when the temperature on the Amplifier falls below the low threshold value.

Severity

Critical

Object affected

Optical Amplifier Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

1. Check for the Amplifier case low temperature alarm.
2. Configure the case temperature above the threshold level.
3. Check for the alarm.

If the alarm persists, contact your next level of support.

9.4 Amplifier Case High Temperature - Trap ID: 1076

Use this procedure to clear ***Amplifier case high temperature*** alarm.

Cause

This alarm is raised when the temperature on the Amplifier crosses the high threshold value.

Severity

Critical

Object affected

Optical Amplifier Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

1. Check for the Amplifier case high temperature alarm.
2. Configure the case temperature below the threshold level.
3. Check for the alarm.

If the alarm persists, contact your next level of support.

9.5 Amplifier Loss Of Input Power - Trap ID: 1077

Use this procedure to clear ***Amplifier Loss of input power*** alarm.

Cause

This alarm is raised when the Input Power on the Amplifier Port becomes less than the set LOS Threshold value.

Severity

Critical

Object affected

Optical Amplifier port

Impact

- When Automatic power shutdown is set as Enable, the alarm is traffic affecting. This alarm triggers the power shutdown on the Amplifier port.
- When Automatic power shutdown is set as Disable, the alarm is traffic affecting due to high noise level addition to the transmitted signal.

Clearing procedure

Perform the following steps to clear the alarm.

1. Ensure that the **Input Power (dBm)** is always above the LOS Threshold value. **LOS Threshold** is a user configurable field; acceptable value ranging from -10 to -40 dBm.
2. To clear a persisting *Amplifier Loss of input power* alarm,
   a. Set the value for **LOS Threshold Deviation** field; acceptable value ranging from -10 to 10 dB.
   b. The alarm will get cleared when the
   c. **Input Power (dBm)** value is greater than or equal to the sum of **LOS Threshold** and **LOS Threshold Deviation** value on the Amplifier port.
   d. Check for the alarm again.

If the alarm still persists, contact your next level of support.

9.6 Amplifier Loss Of Output Power - Trap ID:1078

Use this procedure to clear ***Amplifier Loss of Output power*** alarm.

Cause

This alarm is raised when,

- There is difference in Signal Gain and Set Amplifier Gain is greater than 1. This is applicable when the Operational Mode of the Amplifier port is set to Automatic Gain Control.
- There is difference in Signal Power and Set Amplifier Power is greater than 1. This is applicable when the Operational Mode of the Amplifier port is set to Automatic Power Control.

Severity

Critical

Object affected

Optical Amplifier Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

Perform the following steps to clear the alarm.

1. **Automatic Gain Control**

- Ensure that the **Set Amplifier Gain (dB)** and the **Signal Gain (dB)** values are equal or the difference between the two fields is always less than 1. **Set Amplifier Gain (dB)** is a user configurable field; acceptable value ranging from 15 to 30 dB.
- To clear a persisting *Amplifier Loss of Output power* alarm,
  a. Set the value for **Set Amplifier Gain (dB)** field on the Amplifier port; acceptable value ranging from 15 to 30 dB.
  b. The alarm will get cleared when **Set Amplifier Gain (dB)** and **Signal Gain (dB)** values becomes equal.
  c. Check for the alarm again. If it persists, contact your next level of support.

2. **Automatic Power Control**

- Ensure that the **Set Amplifier Power (dBm)** and the **Signal Gain (dB)** values are equal or the difference between the two fields is always less than 1. **Set**

Amplifier Power (dBm) is a user configurable field; acceptable value ranging from -5 to 21 dBm.

- To clear a persisting *Amplifier Loss of Output power* alarm,
  a. Set the value for **Set Amplifier Power (dBm)** field on the Amplifier port; acceptable value ranging from -5 to 21 dBm.
  b. The alarm will get cleared when **Set Amplifier Power (dBm)** and **Signal Gain (dB)** values becomes equal.
  c. Check for the alarm again.

If the alarm still persists, contact your next level of support.

9.7 Amplifier High Back Reflection - Trap ID: 1079

Use this procedure to clear ***Amplifier High Back Reflection*** alarm.

Cause

This alarm is raised when the back reflection is above threshold due to fibre cut.

Severity

Critical

Object affected

Optical Amplifier

Impact

The impact of the alarm is service affecting.

Clearing procedure

1. Check for the Amplifier High Back Reflection alarm and ensure there is a proper connectivity in the fibre.
2. Ensure that the back reflection is below threshold level.
3. Check for the alarm.

If the alarm persists, contact your next level of support.

9.8 Amplifier Loss Of Input Power Stage Two - Trap ID: 1080

Use this procedure to clear ***Amplifier Loss Of Input Power Stage Two*** alarm.

Cause

This alarm is raised when there is loss of input power threshold for stage two. This is applicable only for Mid stage-Variable Gain (MS-VG) amplifiers.

Severity

Critical

Object affected

Optical Amplifier Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

1. Check for the Amplifier Loss Of Input Power Stage Two alarm.
2. Ensure that the input power is above the threshold level. (Threshold value is -28dBm).
3. Check for the alarm.

If the alarm persists, contact your next level of support.

9.9 Amplifier Loss Of Output Power Stage Two - Trap ID:1081

Use this procedure to clear ***Amplifier Loss Of Output Power Stage Two*** alarm.

Cause

This alarm is raised when there is loss of output power threshold for stage two. This is applicable only for Mid stage-Variable Gain (MS-VG) amplifiers.

Severity

Critical

Object affected

Optical Amplifier

Impact

The impact of the alarm is service affecting.

Clearing procedure

1. Check for the Amplifier Loss Of Output Power Stage Two alarm.
2. Ensure that the output power is above the threshold level. (Threshold value is 0.5 dB deviation from set gain).
3. Check for the alarm.

If the alarm persists, contact your next level of support.

9.10 Amplifier Output Power Out Of Range - Trap ID:1112

Use this procedure to clear ***Amplifier Output Power Out Of Range*** alarm.

Cause

Output signal from the EDFA is below the LOS threshold which has been defined for EDFA.

Severity

Critical

Object affected

Optical amplifier port

Impact

Traffic failure has there is no output from the EDFA.

Clearing procedure

To clear this alarm,

1. Check the amplifier alarms, to see if there is a loss of input power.
2. The output of an EDFA can go down if the input is down.
3. Rectify the issues in input power.

If the alarm persists, contact next level of support.

9.11 Amplifier Input Power Out of Range - Trap ID:1113

Use this procedure to clear ***Amplifier Input Power Out of Range*** alarm.

Cause

Input signal from the EDFA is below LOS threshold which has been defined for the EDFA.

Severity

Critical

Object affected

Optical amplifier port

Impact

Traffic failure has there is no input to the EDFA.

Clearing procedure

To clear this alarm, check for the fiber path to correct the cause of low input power.

If the alarm persists, contact next level of support.

9.12 Amplifier Low Input Power - Trap ID:1114

Use this procedure to clear ***Amplifier Low Input Power*** alarm.

Cause

Alarm raised when the input signal to the EDFA is below a defined threshold.

Severity

Critical

Object affected

Optical amplifier port

Impact

Traffic failure as the input signal to the EDFA is below a threshold which would cause errors.

Clearing procedure

To clear this alarm, check for the fiber path to correct the cause of low input power.

If the alarm persists, contact next level of support.

9.13 Amplifier Degraded Input Power - Trap ID:1115

Use this procedure to clear ***Amplifier Degraded Input Power*** alarm.

Cause

Alarm raised when the input signal to the EDFA is below a defined threshold. This threshold is different from the low input power threshold.

Severity

Critical

Object affected

Optical amplifier port

Impact

Traffic failure as the input signal to the EDFA is below a threshold which causes error.

Clearing procedure

To clear this alarm, check for the fiber path to correct the cause of low input power.

If the alarm persists, contact next level of support.

9.14 Amplifier Degraded Output Power - Trap ID:1116

Use this procedure to clear ***Amplifier Degraded Output Power*** alarm.

Cause

Alarm raised when the output signal from the EDFA is below a defined threshold.

Severity

Critical

Object affected

Optical amplifier port

Impact

Traffic failure as the output signal from the EDFA is below a threshold which would cause errors.

Clearing procedure

To clear this alarm,

1. Low output power would mean lower input signal value
2. Check for the fiber path to correct the cause of the low input power
3. Increase the gain of the EDFA in case the input signal has gone below a certain value

If the alarm persists, contact next level of support.

9.15 Amplifier pump over current at stage two - Trap ID:1255

This procedure is used to clear ***Amplifier pump over current at stage two*** alarm.

Cause

Alarm is specific to multi-stage amplifier cards. Alarm is raised when pump current to the second stage EDFA exceeds a preset threshold in software.

Severity

Critical

Object affected

Optical amplifier port

Impact

The impact of the alarm causes failure in the pump of the second stage EDFA amplifier. The alarm is an indication that the pump laser can get damaged due to excessive current being drawn.

Clearing procedure

To clear this alarm,

1. Increase the input power to the amplifier, so that the pump does not need a large amount of power to achieve the gain, else.
2. Reduce the gain required to be achieved by the EDFA.

If the alarm persists, contact next level of support.

9.16 APR Triggered - Laser is shutdown - Trap ID:1253

This procedure is used to clear ***APR Triggered - Laser is shutdown*** alarm.

Cause

Alarm is raised against amplifier ports which are configured as pairs for APR implementation on the node.

When a LOS happens in a pre-amplifier connected to a DWDM link then the paired booster amplifier output signal is shutoff and the alarm is raised.

Severity

Major

Object affected

Optical amplifier port

Impact

The impact of alarm causes a failure in the pump of the second stage EDFA amplifier. The pump laser can get damaged due to excessive current being drawn.

Clearing procedure

To clear this alarm,

1. Clear the fault on the pre-amplifier.
2. It will clear the alarm on the paired booster amplifier and vice-versa.

If the alarm persists, contact next level of support.

9.17 Channel Attenuation Out Of Range - Trap ID:1225

This procedure is used to clear ***Channel Attenuation Out of Range*** alarm.

Cause

- Alarm is raised against a particular lambda connection where power balancing is enabled.
- When the channel power is attenuated to its maximum value and still the power level balancing is not achieved.
- When the attenuation in the channel is reduced to its lowest value and still the power balancing is not achieved.

Severity

Critical

Object affected

DWDM channel

Impact

Traffic impact due to too much power or too low power in the lambda connection.

Clearing procedure

To clear this alarm,

1. Correct the cause for wrong input power to the channel.
2. Check the amplifier gain in the path to see whether any amplifier is either amplifying the signal too much, or not able to amplify the signal due to some other reasons.
3. Check the attenuation levels along the path to see whether any specific component in the DWDM channel path is adding a lot of attenuation to the signal.

If the alarm persists, contact next level of support.

9.18 Channel Power Out Of Range - Trap ID:1226

This procedure is used to clear ***Channel Power Out of Range*** alarm.

Cause

Alarm is raised when the channel power is beyond the regulation range defined for performing the power balancing. Regulation range is a range of power values between which the output power balancing algorithm will operate.

Severity

Critical

Object affected

DWDM channel

Impact

Affects power balancing of the channel.

Clearing procedure

To clear this alarm, correct the attenuation in the channel path, so that the channel power comes within the regulation range.

If the alarm persists, contact next level of support.

9.19 Channel Power Control Failure- Trap ID:1228

This procedure is used to clear ***Channel Power Control Failure*** alarm.

Cause

Alarm is raised when automatic power balancing action fails to correct the power to the levels which are expected.

Severity

Critical

Object affected

DWDM channel

Impact

Power balancing is done to make sure that downstream channels do not get saturated due to excess power on one of the channels.

Clearing procedure

1. Correct the condition which is causing the power balancing failure.

2. If a channel has failed due to a fiber cut somewhere else in the network then it needs to be traced and corrected.
3. Alarm will clear only when the channel comes back into regulation range or automatic power balancing feature is disabled on that channel.

If the alarm persists, contact next level of support.

9.20 CFPHwFailure - Trap ID:1322

This procedure is used to clear ***CFPHwFailure*** alarm.

Cause

The CFP pluggable as hardware failure.

Severity

Critical

Object affected

MSACFP

Impact

The impact of the alarm is service affective.

Clearing procedure

To clear this alarm, plug in new working CFP hardware or recover hardware fault.
If the alarm persists, contact next level of support.

9.21 CFPMultiFailure - Trap ID:1324

This procedure is used to clear ***CFPMultiFailure*** alarm.

Cause

Failure of CFP

Severity

Critical

Object affected

MSACFP

Impact

The impact of the alarm is service affective.

Clearing procedure

To clear this alarm, wait till all faults recover.

9.22 CFPTempFailure - Trap ID:1323

This procedure is used to clear ***CFPTempFailure*** alarm.

Cause

When the temperature of CFP exceeds safe operating temperature.

Severity

Critical

Object affected

MSACFP

Impact

The impact of the alarm is service affective.

Clearing procedure

To clear this alarm, wait till the temperature of CFP falls within the safe operating temperature range.

If the alarm persists, contact next level of support.

9.23 Forced Switch Active - Trap ID:1108

This procedure helps you clear the ***Forced Switch Active*** alarm.

Cause

This alarm is raised when user issues Forced Switch external command.

Severity

Minor

Object affected

DWDM Channel

Impact

The impact of the alert is non-service affecting. Forced switch to channel has less priority than lockout. Traffic will be switched to protect line even if signal fail or signal degrade conditions exist.

Clearing procedure

To clear this alarm,

1. After completion of maintenance, click **DWDM > Configuration** in the navigation menu.
2. Click **Lambda Protection.** Select the connection ID on which the alarm is present and click **release** button.

If any alarm persists, contact your next level of support.

9.24 FPU Lockout of Protection - Trap ID:943

Use this procedure to clear ***FPU Lockout of protection*** alarm.

Cause

This alarm is raised when the user issues **Lockout Protection** external command on FPU card.

Severity

Critical

Object affected

Card_FPU

Impact

This alarm is service affecting if the work card fails.

Clearing procedure

To clear this alarm, check for the *FPU Lockout of Protection* alarm and apply **Release** command.

If the alarm persists, contact your next level of support.

9.25 FPU Lockout of protection - Trap ID:1259

This procedure is used to clear ***FPU Lockout of Protection*** alarm.

Cause

User initiated command on the FPU. The command is given from the node UI.

Severity

Critical

Object affected

FPU protection

Impact

The FPU will no longer switch to the protect path when a failure happens on the work path.

Clearing procedure

Apply the clear command from the node UI.

If the alarm persists, contact next level of support.

9.26 FPU Forced Switch to protect port - Trap ID:944

Use this procedure to clear ***FPU Forced Switch to protect port*** alarm.

Cause

This alarm is raised when the user issues **Forced Switch to Protect** external command.

Severity

Critical

Object affected

Card_FPU

Impact

This alarm is service affecting when there is fail in Protect path.

Clearing procedure

To clear this alarm, check for the *FPU Forced Switch to protect port* alarm and apply **Release** command.

If the alarm persists, contact your next level of support.

9.27 FPU Forced Switch to protect port - Trap ID:1260

This procedure is used to clear ***FPU Forced Switch to protect port*** alarm.

Cause

User initiated command on the FPU. The command is given from the node UI.

Severity

Critical

Object affected

FPU protection

Impact

The impact of the alarm causes traffic in the work path to switch over to the protect path. If the traffic is already present in the protect path then it will remain in the protect path. In case of LOS on the protect path, traffic will not switch back to work path.

Clearing procedure

Apply clear command from the node UI.

If the alarm persists, contact next level of support.

9.28 FPU Forced Switch to work port - Trap ID:945

Use this procedure to clear ***FPU Forced Switch to work port*** alarm.

Cause

This alarm is raised when the user issues **Forced Switch to Working** external command.

Severity

Critical

Object affected

Card_FPU

Impact

This alarm will be traffic affecting during the switchover operation.

Clearing procedure

To clear this alarm, check for the *FPU Forced Switch to work port* alarm and apply **Release** command.

If the alarm persists, contact your next level of support.

9.29 FPU Forced Switch to work port - Trap ID:1261

This procedure is used to clear ***FPU Forced Switch to work port*** alarm.

Cause

User initiated command on the FPU. The command is given from the node UI.

Severity

Critical

Object affected

FPU protection

Impact

The impact of the alarm causes traffic in the protect path to switch to work path. If the

traffic is already present in the work path then it will remain in the work path. In case of LOS on the work path traffic will not switch back to the protect path.

Clearing procedure

Apply the clear command from the node UI.

If the alarm persists, contact next level of support.

9.30 FPU Switched to protect - Trap ID:946

Use this procedure to clear ***FPU Switched to protect*** alarm.

Cause

This alarm is raised when the user issues **Forced Switch to Protect** external command.

Severity

Critical

Object affected

Card_FPU

Impact

This alarm is service affecting when there is fail in protect path.

Clearing procedure

To clear this alarm, check for the *FPU Forced Switch to protect* alarm and apply **Release** command.

If the alarm persists, contact your next level of support.

9.31 Lockout Active - Trap ID:1107

This procedure helps you clear the ***Lockout Active*** alarm.

Cause

This alarm is raised when user issues LockOutofProtection external command.

Severity

Minor

Object affected

DWDM Channel

Impact

The impact of the alarm is non-service affecting. In case of LockOut Of Protection, traffic will not be switched to protect line even SF/SD conditions exists on work channel.

Clearing procedure

To clear this alarm,

1. After completion of maintenance, click **DWDM > Configuration** in the navigation menu.
2. Click **Lambda Protection.** Select the connection ID on which the alarm is present and click **release** button.

If any alarm persists, contact your next level of support.

9.32 Manual Switch Active - Trap ID:1109

This procedure helps you clear the ***Manual Switch Active*** alarm.

Cause

This alarm is raised when user issues Manual Switch external command. Manual switch to channel. Signal fail or signal degrade conditions can preempt this command.

Severity

Minor

Object affected

DWDM Channel

Impact

The impact of the alert is non-service affecting. Manual switch to channel has less priority than Forced Switch. Traffic will not be switched to protect line if signal fail or signal degrade conditions exist.

Clearing procedure

To clear this alarm,

1. After completion of maintenance, click **DWDM > Configuration** in the navigation menu.
2. Click **Lambda Protection**. Select the connection ID on which the alarm is present and click **release** button.

If any alarm persists, contact your next level of support.

9.33 MSA Module Not Present - Trap ID:1082

Use this procedure to clear ***MSA Module Not Present*** alarm.

Cause

This alarm is raised when the MSA module is not present.

Severity

Critical

Object affected

Optical Amplifier

Impact

The impact of the alarm is service affecting.

Clearing procedure

1. Check for the MSA Module Not Present alarm
2. Ensure that the module access works fine.
3. Check for the alarm.

If the alarm persists, contact your next level of support.

9.34 Pluggable optics Failure - Trap ID:1147

This procedure helps you clear the ***Pluggable Optics Failure*** alarm.

Cause

Alarm raised when the optics module encounters a hardware failure. Alarm specific to high rate optics like CFP/CFP2/QSFP28.

Severity

Critical

Object affected

MSACFP

Impact

Traffic failure as optics is not available for transmission in case the traffic is not protected. If traffic is protected, switching happens as LOS will be detected.

Clearing procedure

To clear this alarm,

1. Alarm indicates a hardware failure in the optics.
2. Replace the optics with working optics.

If the alarm persists, contact next level of support.

9.35 Pluggable optics missing or removed - Trap ID:1146

This procedure is used to clear ***Pluggable optics missing or removed*** alarm.

Cause

Alarm raised when the optics is removed from the card. Alarm specific to high rate optics like CFP/CFP2/QSFP28.

Severity

Critical

Object affected

MSACFP

Impact

Traffic failure as optics is not available for transmission in case the traffic is not protected. If traffic is protected, switching happens as LOS will be detected.

Clearing procedure

To clear this alarm,

1. Check for the physical presence of the optics in the card, if removed, restore the same to clear the alarm.
2. If optics has been removed as part of a replacement procedure, inserting new optics of the same type will clear the alarm automatically.
3. If no plan to use the port, delete the optics image from the inventory page to clear the alarm.

If the alarm persists, contact next level of support.

9.36 Pluggable optics Unknown - Trap ID:1148

This procedure is used to clear ***Pluggable optics Unknown*** alarm.

Cause

Optics parameters which are read from the device are not understood by the software or the optics is not programmed correctly.

Severity

Critical

Object affected

MSACFP

Impact

Impact of alarm is traffic affecting as the optics will not work properly.

Clearing procedure

To clear this alarm,

1. Alarm indicates a hardware failure in the optics
2. Replace the optics with working optics of approved vendor.

If the alarm persists, contact next level of support.

9.37 Pluggable optics Mismatch - Trap ID:1149

This procedure is used to clear ***Pluggable optics Mismatch*** alarm.

Cause

Alarm is raised when the parameters which are detected by software for optics like reach, type are mismatched from what is read from the optics hardware. Issue happens when optics is replaced and the correct type is not used.

Severity

Critical

Object affected

MSACFP

Impact

Traffic affecting as the optics used is incorrect.

Clearing procedure

To clear this alarm, replace the optics with the correct type.

If the alarm persists, contact next level of support.

9.38 Protection Switch Active - Trap ID:1110

This procedure helps you clear the ***Protection Switch Active*** alarm.

Cause

This alarm is raised when the traffic switches from work to protect on signal fail or signal degrade on protect channel.

Severity

Warning

Object affected

DWDM Channel

Impact

The impact of the alert is non-service affecting.

Clearing procedure

To clear this alarm,

1. Apply clearing procedures for which this protection switching occurred.
2. On successful clearing procedures and after WTR time this alarm should get cleared. Determine if there are any Signal fail or Signal degrade alarm present.

If any alarm persists, contact your next level of support.

9.39 Signal Degrade - Trap ID:1266

This procedure is used to clear ***Signal Degrade*** alarm

Cause

Alarm is raised against the FPU work/protect port, when the input power is less than the threshold defined for the signal degrade on that FPU port

Severity

Critical

Object affected

DWDM port

Impact

Traffic running on the port with this alarm present displays errors.

Clearing procedure

The alarm will be cleared when the input power is higher than the degrade threshold + a hysteresis value which is configured against the port.

If the alarm persists, contact next level of support.

9.40 Signal Fail On Protect - Trap ID:1184

This procedure is used to clear ***Signal Fail on Protect*** alarm.

Cause

Alarm is raised when there is a signal failure on the protect port of the FPU.

Severity

Critical

Object affected

Card_FPU

Impact

Traffic cannot switch to the protect path. Traffic running on work path will continue to run on the work path.

Clearing procedure

To clear this alarm, check the fiber connected to the protect port and correct the cause for the low power/LOS on the protect port.

If the alarm persists, contact next level of support.

9.41 Signal Fail On Protect - Trap ID:1262

This procedure is used to clear ***Signal Fail on Protect*** alarm.

Cause

Alarm raised when there is a signal failure on the protect port of the FPU.

Severity

Critical

Object affected

FPU protection

Impact

Traffic cannot switch to the protect path. Traffic running on work path will continue to run on the work path.

Clearing procedure

Check the fiber connected to the protect port and correct the cause for the low power or LOS on the protect port.

If the alarm persists, contact next level of support.

9.42 Signal Fail on Work - Trap ID:1185

This procedure is used to clear ***Signal Fail on Work*** alarm.

Cause

Alarm raised when there is a signal failure on the work port of the FPU.

Severity

Critical

Object affected

Card_FPU

Impact

Traffic cannot switch to the protect path. Traffic running on work path will continue to run on the work path.

Clearing procedure

To clear this alarm, check the fiber connected to the Work port and correct the cause for the low power/LOS on the protect port.

If the alarm persists, contact next level of support.

9.43 Signal Fail on Work - Trap ID:1263

This procedure is used to clear ***Signal Fail on Work*** alarm.

Cause

Alarm raised when there is a signal failure on the work port of the FPU.

Severity

Critical

Object affected

FPU protection

Impact

Traffic cannot switch to the protect path. Traffic running on work path will continue to run on the work path.

Clearing procedure

Check the fiber connected to the protect port and correct the cause for the low power or LOS on the protect port.

If the alarm persists, contact next level of support.

9.44 Signal Fail - Trap ID:1227

This procedure is used to clear ***Signal Fail*** alarm.

Cause

Alarm indicates signal failure on the common port of the FPU.

Common port is connected to the transponder or interface which needs to be protected by the FPU.

Severity

Critical

Object affected

Card_FPU

Impact

The impact of the alarm is traffic affecting as the link is not a protected. The link is a intra chassis link and does not go over the network.

Clearing procedure

To clear this alarm, check the common port connection and ensure that the fiber connection is proper.

If the alarm persists, contact next level of support.

This page is intentionally left blank

10 L2 alarms

This chapter describes L2 based alarms raised on Tejas Network Elements and the procedures to clear these alarms.

10.1 CCM Interval Mismatch - Trap ID:663

Use this procedure to clear the ***CCM Interval Mismatch*** alarm.

Cause

This alarm is raised when MEP receives a CCM frame with valid MD Level and a valid MAID, but at a CCM interval different than local end configured interval.

Severity

Critical

Object affected

MEPs against ports, PBT tunnels and services over PBT tunnels.

Impact

This alarm is traffic affecting only when the protection switching due to CFM does not happen in case there is a mismatch between the CCM intervals.

Clearing procedure

To clear the alarm,

1. Check the CCM interval configured across the Maintenance Association.
2. Check the CCM interval of the associated MEP on the end-point where the remote MEP is configured.

NOTE: This alarm clears when a MEP receives three consecutive CCM frames with correct MD Level, MAID and CCM interval. Check if the *CCM Interval Mismatch* alarm is cleared.

If the alarm persists, contact your next level of support.

10.2 Connectivity Check Failed - Trap ID:658

Use this procedure to clear ***Connectivity Check Failed*** alarm.

Cause

A MEP does not receive CCM frames from a peer MEP for an interval equal to 3 times the CCM transmission period.

Severity

Critical

Object affected

MEP

Clearing procedure

To clear this alarm,

1. Check whether the physical connectivity and Maintenance Association (MA) Domain is proper on both sides.
2. Trigger a Loop Back Message (LBM) to the remote MEP.
3. If there is no response, trigger a Link Trace Message (LTM) to the remote MEP to isolate the fault.
4. At the remote end, check if all the associated entities have been enabled.

If the alarm persists, contact your next level of support.

10.3 FDB Limit Reached - Trap ID:686

Use this procedure to clear the ***FDB Limited Reached*** alarm.

Cause

This alarm is raised when the number of learnt MAC address reaches the configured limit in a service.

Severity

Critical

Object affected

EVC

Impact

No more entries is learnt. Any traffic which has to be forwarded to unlearnt MAC address broadcasted to all ports in the service. The network throughput gets affected.

Clearing procedure

To clear the alarm, understand the number of MAC address required to be learnt and appropriately adjust the FDB limit.

If the alarm persists, contact your next level of support.

10.4 LAG Capacity Changed- Trap ID: 755

Use this procedure to clear ***LAG Capacity Changed*** alarm.

MIB Name

LAG Capacity Changed.

Cause

Capacity of LAG changes due to following reasons:

1. Link up/link down occurred on any of the existing LAG member ports.
2. Addition/deletion of one more ports to the LAG ports.

Severity

Major

Objects Affected

LAG Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

In cases where member ports have become link down, the link has to be restored.

10.5 LAG Link Down - Trap ID:842

Use this procedure to clear ***LAG Link Down*** alarm.

MIB name

LAG Link Down.

Cause

LAG link down alarm raises when all the LAG member ports are link down.

Severity

Major

Object affected

LAG Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Check and correct for loose/faulty cable between the Ethernet ports on the local node and client.
2. Check that the client Ethernet port is enabled.
3. Link Down condition clears when there is no signal defect detected at local and remote ends of the link.

If the alarm persists, contact next level of support.

10.6 Loop Detected - Trap ID:664

Use this procedure to clear the ***Loop Detected*** alarm.

Cause

MEP receives CCM frame with MEPID, MAID, CCM interval, MD level and MAC address same as of its own MEP.

Severity

Critical

Object affected

MEP

Impact

The impact of this alarm is service affecting.

Clearing procedure

To clear the alarm,

1. Check the loop detection alarm.
2. Remove the loop from the network.
3. Alarm is cleared when no such packets are received in three consecutive frames.

If the alarm persists, contact your next level of support.

10.7 Loss of Signal - Trap ID:611

Use this procedure to clear the ***Loss of Signal*** alarm.

Cause

This alarm is raised when,

- There is a fiber cut (or)
- The received signal level drops below an implementation determined threshold

Severity

Critical

Object affected

Ethernet Port

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear the alarm,

1. Determine if the cable is faulty and replace the cable.
2. Check if the *Loss of Signal* alarm on Ethernet port is cleared.

If the alarm persists, contact your next level of support.

10.8 Misconnection Detected on OAM Ports - Trap ID:1092

Use this procedure to clear ***Misconnection Detected on OAM Ports*** alarm.

Cause

The alarm is raised when loopback is detected on VLAN interface.

Severity

Major

Object affected

System

Impact

The impact of the alarm is no-service affected.

Clearing procedure

To clear this alarm, remove the loopback on VLAN Interface.

If the alarm persists, contact your next level of support.

10.9 Multiple RPL Owners Configured - Trap ID:660

Use this procedure to clear the ***Multiple RPL Owners Configured*** alarm.

Cause

This alarm is raised when multiple RPL ports are configured in the ringlet.

Severity

Critical

Object affected

Ringlet

Impact

ERP configured is not usable.

Clearing procedure

To clear the alarm,

1. Identify the correct RPL port in the ringlet.
2. Delete the configuration on other nodes where RPL is configured and re-create them without RPL.

If the alarm persists, contact your next level of support.

10.10 No RPL Owner Configured - Trap ID:659

Use this procedure to clear the ***No RPL Owner Configured*** alarm.

Cause

This alarm is raised when no RPL is configured on the ERP ringlet.

Severity

Critical

Object affected

Ringlet

Impact

ERP configured is not usable.

Clearing procedure

To clear the alarm,

1. Identify the RPL port in the ringlet.
2. Delete the ringlet configuration on the identified node and re-create the ringlet with RPL port notified.

If the alarm persists, contact your next level of support.

10.11 PacketTrunk OperStatus Down - Trap ID:694

Use this procedure to clear the ***PacketTrunk OperStatus Down*** alarm.

Cause

This alarm is raised when an operational packet trunk goes down.

Severity

Minor

Object affected

Packet Trunk

Impact

The services created in NMS on the packet trunk may not get activated.

Clearing procedure

To clear the alarm,

Check for any faults or mismatch in LLDP settings on both the ends of the packet trunk and correct them. This alarm clears when the LLDP messages are received correctly and adjacency is established.

If the alarm persists, contact your next level of support.

10.12 Port Mirroring Active - Trap ID:688

Use this procedure to clear the ***Port Mirroring Active*** alarm.

Cause

Port Mirroring Session is created.

Severity

Minor

Object affected

Data Port

Impact

The impact of this alarm is traffic affecting. Traffic from the source port is mirrored on the destination port.

Clearing procedure

To clear this alarm,

Remove the destination port of Port Mirroring Session through explicit user command.

If the alarm persists, contact next level of support.

10.13 Remote and Local IP Match - Trap ID:693

Use this procedure to clear the ***Remote and Local IP Match*** alarm.

Cause

This alarm is raised when the remote IP and local IP are same when packet trunk is dynamically discovered.

Severity

Minor

Object affected

Packet Trunk

Impact

Indicates a mis-connection. This trunk cannot be used in NMS for service creation.

Clearing procedure

To clear the alarm,

Check the physical connectivity and correct it. The alarm clears when correct connectivity is made.

If the alarm persists, contact your next level of support.

10.14 Remote Defect Indication - Trap ID:662

Use this procedure to clear the ***Remote Defect Indication*** alarm.

Cause

This alarm is raised when received RDI bit on a MEP indicates a problem on the remote MEP.

Severity

Critical

Object affected

MEP

Impact

Indicates fault on the remote end. If not resolved, this may lead to traffic loss in case of another fault.

Clearing procedure

To clear the alarm,

1. Clear the fault existing on the remote end MEP.
2. Check the RMEP ID and MEP ID on both the ends and ensure correctness.

If the alarm persists, contact your next level of support.

10.15 Ringlet External Command Active - Trap ID:1183

This procedure is used to clear **Ringlet External Command Active** alarm.

Cause

The alarm is raised due to activation of external command in one or more nodes in the ringlet

Severity

Critical

Object affected

Ringlet

Impact

The impact of the alarm is service affecting.

Ring is in protected state

Clearing procedure

To clear this alarm, give clear External Command on Ringlet.

If the alarm persists, contact next level of support.

10.16 Traffic Field Mismatch - Trap ID:689

This procedure is used to clear ***Traffic Field Mismatch*** alarm.

Cause

This alarm is raised on the group when some members are operationally down.

Severity

Critical

Object affected

MEP

Impact

Impact of the alarm is service affecting.

Clearing procedure

To clear this alarm,

1. Find out which Rx/Tx Link went down.
2. Clear the Link fault.

If the alarm persists, contact next level of support.

10.17 Unexpected MAID - Trap ID:661

Use this procedure to clear ***Unexpected MAID*** alarm on a tunnel group.

Cause

This alarm is raised when there is short Maintenance Association (MA) name mismatch on either end of the Maintenance End Point (MEP).

Severity

Critical

Object affected

MEPs against ports, PBT tunnels and services over PBT tunnels

Impact

The impact of the alarm is service affecting.

Clearing procedure

This alarm is cleared when the short Maintenance Association (MA) name is same on both ends of the MEP.

If the alarm persists, contact your next level of support.

10.18 Unexpected MEPID - Trap ID:665

Use this procedure to clear the **Unexpected MEPID** alarm.

Cause

A MEP receives a CCM frame with correct MEG Level, correct MEG ID but with unexpected MEPID.

Severity

Critical

Object affected

MEPs against ports, PBT tunnels and services over PBT tunnels

Impact

The impact of the alarm is service affecting.

Clearing procedure

To clear the alarm,

1. Check MEPID of remote MEP. MEPID of the remote MEP should be part of remote MEPIDs of the local MEP.
2. Alarm is cleared when no mismatch in MEPID is detected in three consecutive frames.

If the alarm persists, contact the next level of support.

10.19 Unexpected MD Level - Trap ID:666

Use this procedure to clear the ***Unexpected MD Level*** alarm.

Cause

This alarm is raised on the group when there is misconfiguration or a leak in the CFM domains. The MEP has detected CFM frames at a lower MD level.

Severity

Critical

Object affected

MEPs against ports, PBT tunnels and services over PBT tunnels

Impact

Traffic protected by the MEP is down.

Clearing procedure

To clear the alarm,

Identify the misconfiguration or the leak and correct it. The alarm clears when misconfiguration or leak of CFM domains are corrected.

If the alarm persists, contact your next level of support.

11 MPLS-TP Alarms

This chapter gives details of MPLS-TP related alarms and its clearing procedure.

11.1 Misconfiguration of PseudowireGroup-Trap ID: 1175

Use this procedure to clear ***Misconfiguration of PseudowireGroup*** alarm.

Cause

This alarm is raised when configuration error occurs, such as when PseudoWireGroup is configured in MASTER mode and signalling method is in STANDBY mode, but receives STANDBY as remote status.

Severity

Critical

Object affected

PseudoWireGroup

Impact

The impact of the alarm is traffic affecting.

Clearing procedure

Change the PseudowireGroup Protection Switch Selection at remote end to SLAVE mode.

11.2 Object creation in hardware failed (Tunnel)-Trap ID: 1173

Use this procedure to clear ***Object creation in hardware failed*** alarm.

Cause

This alarm is raised when creation of tunnel fails in hardware due to lack of resource, or because of Hash table failure.

Severity

Critical

Object affected

MPLSTunnel

Impact

The impact of the alarm is no-service affected.

Clearing procedure

Manually delete the tunnel and try to recreate it.

11.3 Object creation in hardware failed (Pseudowire)-Trap ID: 1172

Use this procedure to clear ***creation in hardware failed*** alarm.

Cause

This alarm is raised when creation of pseudowire fails in hardware due to lack of resource, or because of Hash table failure.

Severity

Critical

Object affected

PseudoWire

Impact

The impact of the alarm is no-service affected.

Clearing procedure

Manually delete the Pseudowire and try to recreate it.

11.4 Protection Switching is Incomplete - Trap ID:669

Use this procedure to clear ***Protection Switching Incomplete*** alarm on a tunnel group.

Cause

This alarm is raised when,

- Higher priority alarm 1 above is present (or)
- Near end requested (selected) signal is different from far end bridged signal

Severity

Critical

Object affected

Protection Group

Impact

Traffic will be affected on the tunnel group.

Clearing procedure

To clear this alarm, check and clear higher priority alarm 1.

If the alarm persists, contact your next level of support.

11.5 Pseudowire Down (Trap ID: 1132)

Use this procedure to clear ***Pseudowire Down*** alarm.

Cause

This alarm is raised when a fault is reported on the PseudoWire on which Pseudowire Status Messaging (PWSM) is set as enabled. Faults are raised based on TunnelGroup Status (indirectly Tunnel MEP Status) or Attachment Circuit link failure.

Severity

Critical

Object affected

PseudoWire

Impact

The impact of the alarm is traffic affecting.

Clearing procedure

To clear this alarm,

1. Check the status of MEP on the Tunnels in a TunnelGroup. At least one Tunnel path (Work Tunnel or Protect Tunnel) needs to be error free, so that the fault on the Pseudowire can be cleared.
2. If Pseudowire is down due to attachment circuit link failure, then attachment circuit link needs to be restored.

If the alarm persists, contact your next level of support.

11.6 Remote Defect Indication (Trap ID: 662)

Use this procedure to clear ***Remote Defect Indication*** alarm.

Cause

This alarm is raised when the remote MEP does not receive or stops receiving CC packets from local MEP. This indicates uni-directional link failure. Other causes include:

- Configuration error
- Link down between local MEP and remote MEP
- Because of congestion, there may be CC packet drops due to other traffic of same priority at high rate.
- FPGA failure in the local card or remote card.

Severity

Critical

Object affected

MEP

Impact

The impact of this alarm may be traffic affecting.

Clearing procedure

To clear this alarm,

1. Correct the configuration. Remote MEP ID at near end should be same as MEP ID at far end.
2. If there is a link down between local MEP and remote MEP, rectify the link.
   - To detect where the problem exists, traverse through all the MIPs obtained from LSP TraceRoute from far end to near end, and trigger LSP Ping from far end.
   - If LSP ping doesn't work at particular MIP and it works for the adjacent MIP towards the near end, then that point is where the problem exists.
3. If the CC failure is due to congestion, this alarm may disappear automatically.
4. If this alarm is toggling, check whether traffic sent with priority '7' is exceeding the configured capacity.
5. If there is FPGA failure in local card or remote card, then replace the card.

If the alarm persists, contact your next level of support.