



Alarm Troubleshooting



Note

The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco ONS 15454 alarm and condition. Tables 2-1 through 2-5 provide lists of ONS 15454 alarms organized by severity. Table 2-6 on page 2-7 provides a list of alarms organized alphabetically. Table 2-7 gives definitions of all ONS 15454 alarm logical objects, which are the basis of the alarm profile list in Table 2-8 on page 2-14. For a comprehensive list of all conditions, refer to the *Cisco ONS SONET TL1 Command Guide*.

An alarm's troubleshooting procedure applies to both the Cisco Transport Controller (CTC) and TL1 version of that alarm. If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call the Cisco Technical Assistance Center (1 800 553-2447).

More information about alarm profile information modification and downloads are located in the *Cisco ONS 15454 Procedure Guide* Chapter 7, "Manage Alarms."

2.1 Alarm Indexes by Default Severity

The following tables group alarms and conditions by their default severities in the ONS 15454 system. These severities are the same whether they are reported in the CTC Alarms window severity (SEV) column or in TL1.



Note

The CTC default alarm profile contains some alarms or conditions that are not currently implemented but are reserved for future use.



Note

The CTC default alarm profile in some cases contains two severities for one alarm (for example, MJ/MN). The ONS 15454 platform default severity comes first (in this example, MJ), but the alarm can be demoted to the second severity in the presence of a higher-ranking alarm. This is in accordance with Telcordia GR-474.

2.1.1 Critical Alarms (CR)

Table 2-1 alphabetically lists ONS 15454 Critical alarms.

Table 2-1 ONS 15454 Critical Alarm Index

2.8.28 AUTOLSROFF, page 2-45	2.8.171 LOA, page 2-138	2.8.237 MEA (AIP), page 2-179
2.8.39 AWG-FAIL, page 2-50	2.8.175 LOF (DS3), page 2-141	2.8.238 MEA (BIC), page 2-179
2.8.40 AWG-OVERTEMP, page 2-51	2.8.176 LOF (EC1), page 2-142	2.8.239 MEA (EQPT), page 2-181
2.8.43 BKUPMEMP, page 2-52	2.8.177 LOF (OCN), page 2-143	2.8.240 MEA (FAN), page 2-183
2.8.57 COMIOXC, page 2-64	2.8.178 LOF (TRUNK), page 2-143	2.8.241 MEA (PPM), page 2-183
2.8.64 CTNEQPT-PBPROT, page 2-70	2.8.180 LOM, page 2-144	2.8.244 MFGMEM, page 2-185
2.8.65 CTNEQPT-PBWORK, page 2-71	2.8.181 LOP-P, page 2-145	2.8.262 OPWR-HFAIL, page 2-195
2.8.75 ENCAP-MISMATCH-P, page 2-77	2.8.184 LOS (2R), page 2-147	2.8.264 OPWR-LFAIL, page 2-196
2.8.78 EQPT, page 2-82	2.8.187 LOS (DS3), page 2-149	2.8.269 OTUK-LOF, page 2-199
2.8.79 EQPT-DIAG, page 2-83	2.8.188 LOS (EC1, EC1-12), page 2-150	2.8.277 PLM-P, page 2-204
2.8.80 EQPT-MISS, page 2-83	2.8.191 LOS (ISC), page 2-152	2.8.282 PORT-ADD-PWR-FAIL-LOW, page 2-205
2.8.96 FAN, page 2-97	2.8.193 LOS (OCN), page 2-153	2.8.340 SWMTXMOD, page 2-235
2.8.131 GAIN-LDEG, page 2-115	2.8.194 LOS (OTS), page 2-155	2.8.351 TIM, page 2-242
2.8.132 GAIN-LFAIL, page 2-115	2.8.195 LOS (TRUNK), page 2-156	2.8.353 TIM-P, page 2-243 (for STSTRM)
2.8.134 GE-OOSYNC, page 2-116	2.8.197 LOS-P (OCH), page 2-159	2.8.364 UNEQ-P, page 2-249
2.8.147 HITEMP, page 2-124 (for NE)	2.8.198 LOS-P (OMS, OTS), page 2-161	2.8.372 VOA-HFAIL, page 2-254
2.8.150 I-HITEMP, page 2-126	2.8.199 LOS-P (TRUNK), page 2-163	2.8.374 VOA-LFAIL, page 2-255
2.8.151 IMPROPRMVL, page 2-127	—	—

2.1.2 Major Alarms (MJ)

Table 2-2 alphabetically lists ONS 15454 Major alarms.

Table 2-2 ONS 15454 Major Alarm Index

2.8.15 APSCM, page 2-37	2.8.91 EXTRA-TRAF-PREEMPT, page 2-91	2.8.284 PRC-DUPID, page 2-207
2.8.16 APSCNMIS, page 2-38	2.8.97 FC-NO-CREDITS, page 2-98	2.8.286 PTIM, page 2-208
2.8.42 BAT-FAIL, page 2-51	2.8.99 FEC-MISM, page 2-99	2.8.292 RCVR-MISS, page 2-212
2.8.44 BLSROSYNC, page 2-53	2.8.135 GFP-CSF, page 2-117	2.8.297 RING-ID-MIS, page 2-215
2.8.46 CARLOSS (CE100T), page 2-54	2.8.136 GFP-DE-MISMATCH, page 2-117	2.8.298 RING-MISMATCH, page 2-215

Table 2-2 ONS 15454 Major Alarm Index (continued)

2.8.47 CARLOSS (E100T, E1000F), page 2-54	2.8.137 GFP-EX-MISMATCH, page 2-118	2.8.317 SIGLOSS, page 2-225
2.8.48 CARLOSS (EQPT), page 2-56	2.8.138 GFP-LFD, page 2-118	2.8.325 SSM-FAIL, page 2-231 for double failure
2.8.50 CARLOSS (G1000), page 2-58	2.8.139 GFP-NO-BUFFERS, page 2-119	2.8.345 SYNCLOSS, page 2-238
2.8.51 CARLOSS (GE), page 2-61	2.8.140 GFP-UP-MISMATCH, page 2-119	2.8.346 SYNCPRI, page 2-239
2.8.52 CARLOSS (ISC), page 2-61	2.8.142 HIBATVG, page 2-120	2.8.349 SYSBOOT, page 2-241
2.8.53 CARLOSS (ML100T, ML1000), page 2-62	2.8.156 INVMACADR, page 2-130	2.8.354 TIM-V, page 2-244
2.8.54 CARLOSS (TRUNK), page 2-63	2.8.163 LASERBIAS-FAIL, page 2-134	2.8.355 TPTFAIL (CE100T), page 2-244
2.8.59 CONTBUS-A-18, page 2-66	2.8.174 LOF (DS1), page 2-140	2.8.356 TPTFAIL (FCMR), page 2-244
2.8.60 CONTBUS-B-18, page 2-66	2.8.180 LOM, page 2-144	2.8.357 TPTFAIL (G1000), page 2-245
2.8.61 CONTBUS-IO-A, page 2-67	2.8.182 LOP-V, page 2-145	2.8.358 TPTFAIL (ML100T, ML1000), page 2-245
2.8.62 CONTBUS-IO-B, page 2-68	2.8.186 LOS (DS1), page 2-148	2.8.359 TRMT, page 2-246
2.8.67 DBOSYNC, page 2-73	2.8.228 LWBATVG, page 2-176	2.8.360 TRMT-MISS, page 2-247
2.8.69 DSP-COMM-FAIL, page 2-75	2.8.242 MEM-GONE, page 2-184	2.8.365 UNEQ-V, page 2-251
2.8.70 DSP-FAIL, page 2-75	2.8.260 OPTNTWMIS, page 2-192	2.8.367 UT-COMM-FAIL, page 2-252
2.8.73 Ehibatvg, page 2-76	2.8.273 OUT-OF-SYNC, page 2-201	2.8.368 UT-FAIL, page 2-252
2.8.74 ELWBATVG, page 2-77	2.8.276 PEER-NORESPONSE, page 2-203	2.8.378 WV-L-MISMATCH, page 2-256
2.8.86 E-W-MISMATCH, page 2-87	2.8.278 PLM-V, page 2-205	—

2.1.3 Minor Alarms (MN)

Table 2-3 alphabetically lists ONS 15454 Minor alarms.

Table 2-3 ONS 15454 Minor Alarm Index

2.8.11 APSB, page 2-34	2.8.118 FIBERTEMP-DEG, page 2-110	2.8.243 MEM-LOW, page 2-184
2.8.12 APSCDFLTK, page 2-35	2.8.127 FSTSYNC, page 2-113	2.8.246 NOT-AUTHENTICATED, page 2-186
2.8.13 APSC-IMP, page 2-36	2.8.129 GAIN-HDEG, page 2-113	2.8.261 OPWR-HDEG, page 2-193
2.8.14 APSCINCON, page 2-37	2.8.131 GAIN-LDEG, page 2-115	2.8.263 OPWR-LDEG, page 2-195
2.8.17 APSIMP, page 2-39	2.8.133 GCC-EOC, page 2-116	2.8.268 OTUK-IAE, page 2-198
2.8.18 APS-INV-PRIM, page 2-40	2.8.141 HELLO, page 2-120	2.8.285 PROTNA, page 2-208

Table 2-3 ONS 15454 Minor Alarm Index (continued)

2.8.20 APSMM, page 2-40	2.8.144 HI-LASERBIAS, page 2-121	2.8.287 PWR-FAIL-A, page 2-209
2.8.21 APS-PRIM-SEC-MISM, page 2-41	2.8.145 HI-LASERTEMP, page 2-122	2.8.288 PWR-FAIL-B, page 2-210
2.8.29 AUTORESET, page 2-46	2.8.146 HI-RXPOWER, page 2-123	2.8.289 PWR-FAIL-RET-A, page 2-210
2.8.32 AUTOSW-LOP (VT-MON), page 2-48	2.8.147 HITEMP, page 2-124 (EQPT)	2.8.290 PWR-FAIL-RET-B, page 2-211
2.8.37 AUTOSW-UNEQ (VT-MON), page 2-50	2.8.148 HI-TXPOWER, page 2-125	2.8.313 SFTWDOWN, page 2-224
2.8.38 AWG-DEG, page 2-50	2.8.159 KBYTE-APS-CHANNEL-F AILURE, page 2-133	2.8.314 SH-INS-LOSS-VAR-DEG-HIGH, page 2-224
2.8.45 BPV, page 2-54	2.8.162 LASERBIAS-DEG, page 2-134	2.8.315 SH-INS-LOSS-VAR-DEG-LOW, page 2-225
2.8.55 CASETEMP-DEG, page 2-63	2.8.164 LASEREOL, page 2-135	2.8.318 SNTP-HOST, page 2-226
2.8.58 COMM-FAIL, page 2-65	2.8.165 LASERTEMP-DEG, page 2-135	2.8.325 SSM-FAIL, page 2-231
2.8.66 DATAFLT, page 2-73	2.8.166 LCAS-CRC, page 2-136	2.8.346 SYNCPRI, page 2-239 for EXT-SREF
2.8.71 DUP-IPADDR, page 2-75	2.8.173 LOF (BITS), page 2-139	2.8.347 SYNCSEC, page 2-240
2.8.72 DUP-NODENAME, page 2-76	2.8.179 LO-LASERTEMP, page 2-144	2.8.348 SYNCTHIRD, page 2-240
2.8.76 EOC, page 2-79	2.8.183 LO-RXPOWER, page 2-146	2.8.352 TIM-MON, page 2-243
2.8.77 EOC-L, page 2-81	2.8.185 LOS (BITS), page 2-147	2.8.353 TIM-P, page 2-243 (STSMON)
2.8.84 ERROR-CONFIG, page 2-85	2.8.190 LOS (FUDC), page 2-151	2.8.366 UNREACHABLE-TARGET-POWER, page 2-251
2.8.87 EXCCOL, page 2-89	2.8.196 LOS-O, page 2-157	2.8.371 VOA-HDEG, page 2-253
2.8.90 EXT, page 2-90	2.8.200 LO-TXPOWER, page 2-164	2.8.373 VOA-LDEG, page 2-254
2.8.117 FEPRLF, page 2-109	—	—

2.1.4 NA Conditions

Table 2-4 alphabetically lists ONS 15454 Not Alarmed conditions.

Table 2-4 ONS 15454 NA Conditions Index

2.8.5 ALS, page 2-32	2.8.143 HI-CCVOLT, page 2-121	2.8.258 ODUK-TIM-PM, page 2-191
2.8.7 APC-CORRECTION-SKIPPED, page 2-33	2.8.144 HI-LASERBIAS, page 2-121 for PPM	2.8.259 OOU-TPT, page 2-192
2.8.8 APC-DISABLED, page 2-33	2.8.145 HI-LASERTEMP, page 2-122 for PPM	2.8.265 OSRION, page 2-196

Table 2-4 ONS 15454 NA Conditions Index (continued)

2.8.9 APC-END, page 2-34	2.8.149 HLDOVRSYNC, page 2-125	2.8.270 OTUK-SD, page 2-199
2.8.10 APC-OUT-OF-RANGE, page 2-34	2.8.152 INC-ISD, page 2-128	2.8.271 OTUK-SF, page 2-200
2.8.19 APS-PRIM-FAC, page 2-40	2.8.153 INHSWPR, page 2-128	2.8.272 OTUK-TIM, page 2-200
2.8.22 AS-CMD, page 2-42	2.8.154 INHSWWKG, page 2-129	2.8.274 PARAM-MISM, page 2-201
2.8.23 AS-MT, page 2-43	2.8.155 INTRUSION-PSWD, page 2-129	2.8.275 PDI-P, page 2-201
2.8.24 AS-MT-OOG, page 2-43	2.8.157 IOSCFGCOPY, page 2-132	2.8.283 PORT-MISMATCH, page 2-207
2.8.25 AUD-LOG-LOSS, page 2-44	2.8.158 KB-PASSTHR, page 2-132	2.8.291 RAI, page 2-211
2.8.26 AUD-LOG-LOW, page 2-45	2.8.160 LAN-POL-REV, page 2-133	2.8.299 RING-SW-EAST, page 2-216
2.8.31 AUTOSW-LOP (STSMON), page 2-47	2.8.161 LASER-APR, page 2-134	2.8.300 RING-SW-WEST, page 2-216
2.8.33 AUTOSW-PDI, page 2-48	2.8.167 LCAS-RX-FAIL, page 2-137	2.8.301 RPRW, page 2-216
2.8.34 AUTOSW-SDBER, page 2-49	2.8.168 LCAS-TX-ADD, page 2-137	2.8.302 RUNCFG-SAVENEED, page 2-217
2.8.35 AUTOSW-SFBER, page 2-49	2.8.169 LCAS-TX-DNU, page 2-138	2.8.303 SD (DS1, DS3), page 2-217
2.8.36 AUTOSW-UNEQ (STSMON), page 2-49	2.8.170 LKOUTPR-S, page 2-138	2.8.304 SD (TRUNK), page 2-219
2.8.41 AWG-WARM-UP, page 2-51	2.8.172 LOCKOUT-REQ, page 2-139	2.8.305 SD-L, page 2-219
2.8.56 CLDRESTART, page 2-64	2.8.201 LPBKCRS, page 2-165	2.8.306 SD-P, page 2-220
2.8.63 CTNEQPT-MISMATCH, page 2-69	2.8.202 LPBKDS1FEAC, page 2-166	2.8.307 SD-V, page 2-220
2.8.68 DS3-MISM, page 2-74	2.8.203 LPBKDS1FEAC-CMD, page 2-166	2.8.308 SF (DS1, DS3), page 2-221
2.8.85 ETH-LINKLOSS, page 2-86	2.8.204 LPBKDS3FEAC, page 2-166	2.8.309 SF (TRUNK), page 2-222
2.8.88 EXERCISE-RING-FAIL, page 2-89	2.8.205 LPBKDS3FEAC-CMD, page 2-167	2.8.310 SF-L, page 2-223
2.8.89 EXERCISE-SPAN-FAIL, page 2-90	2.8.206 LPBKFACILITY (CE100T), page 2-167	2.8.311 SF-P, page 2-223
2.8.92 FAILTOSW, page 2-91	2.8.207 LPBKFACILITY (DS1, DS3), page 2-168	2.8.312 SF-V, page 2-223
2.8.93 FAILTOSW-PATH, page 2-92	2.8.208 LPBKFACILITY (EC1), page 2-168	2.8.316 SHUTTER-OPEN, page 2-225
2.8.94 FAILTOSWR, page 2-93	2.8.210 LPBKFACILITY (FC), page 2-169	2.8.319 SPAN-SW-EAST, page 2-227
2.8.95 FAILTOSWS, page 2-95	2.8.211 LPBKFACILITY (FCMR), page 2-169	2.8.320 SPAN-SW-WEST, page 2-227
2.8.98 FE-AIS, page 2-99	2.8.212 LPBKFACILITY (G1000), page 2-169	2.8.321 SQUELCH, page 2-227

Table 2-4 ONS 15454 NA Conditions Index (continued)

2.8.100 FE-DS1-MULTLOS, page 2-100	2.8.213 LPBKFACILITY (GE), page 2-170	2.8.322 SQUELCHED, page 2-229
2.8.101 FE-DS1-NSA, page 2-100	2.8.214 LPBKFACILITY (ISC), page 2-170	2.8.324 SSM-DUS, page 2-231
2.8.102 FE-DS1-SA, page 2-101	2.8.215 LPBKFACILITY (OCN), page 2-171	2.8.326 SSM-LNC, page 2-232
2.8.103 FE-DS1-SNGLLOS, page 2-101	2.8.216 LPBKFACILITY (TRUNK), page 2-171	2.8.327 SSM-OFF, page 2-232
2.8.104 FE-DS3-NSA, page 2-102	2.8.217 LPKTERMINAL (CE100T), page 2-172	2.8.328 SSM-PRC, page 2-232
2.8.105 FE-DS3-SA, page 2-102	2.8.218 LPBKTERMINAL (DS1, DS3), page 2-172	2.8.329 SSM-PRS, page 2-233
2.8.106 FE-EQPT-NSA, page 2-103	2.8.219 LPBKTERMINAL (EC1), page 2-173	2.8.330 SSM-RES, page 2-233
2.8.107 FE-FRCDWKSWBK-SPAN, page 2-104	2.8.220 LPBKTERMINAL (ESCON), page 2-173	2.8.333 SSM-SMC, page 2-233
2.8.108 FE-FRCDWKSWPR-RING, page 2-104	2.8.221 LPBKTERMINAL (FC), page 2-173	2.8.334 SSM-ST2, page 2-234
2.8.109 FE-FRCDWKSWPR-SPAN, page 2-105	2.8.222 LPBKTERMINAL (FCMR), page 2-174	2.8.335 SSM-ST3, page 2-234
2.8.110 FE-IDLE, page 2-105	2.8.223 LPBKTERMINAL (G1000), page 2-174	2.8.336 SSM-ST3E, page 2-234
2.8.111 FE-LOCKOUTOFPR-SPAN, page 2-106	2.8.224 LPBKTERMINAL (GE), page 2-175	2.8.337 SSM-ST4, page 2-234
2.8.112 FE-LOF, page 2-106	2.8.225 LPBKTERMINAL (ISC), page 2-175	2.8.338 SSM-STU, page 2-235
2.8.113 FE-LOS, page 2-107	2.8.226 LPBKTERMINAL (OCN), page 2-175	2.8.339 SSM-TNC, page 2-235
2.8.114 FE-MANWKSWBK-SPAN, page 2-107	2.8.227 LPBKTERMINAL (TRUNK), page 2-176	2.8.341 SWTOPRI, page 2-237
2.8.115 FE-MANWKSWPR-RING, page 2-108	2.8.229 MAN-REQ, page 2-177	2.8.342 SWTOSEC, page 2-237
2.8.116 FE-MANWKSWPR-SPAN, page 2-109	2.8.230 MANRESET, page 2-177	2.8.343 SWTOTHIRD, page 2-237
2.8.119 FORCED-REQ, page 2-110	2.8.231 MANSWTOINT, page 2-177	2.8.344 SYNC-FREQ, page 2-238
2.8.120 FORCED-REQ-RING, page 2-110	2.8.232 MANSWTOPRI, page 2-178	2.8.350 TEMP-MISM, page 2-241
2.8.121 FORCED-REQ-SPAN, page 2-111	2.8.233 MANSWTOSEC, page 2-178	2.8.362 TX-RAI, page 2-248
2.8.122 FRCDSWTOINT, page 2-111	2.8.234 MANSWTOOTHIRD, page 2-178	2.8.363 UNC-WORD, page 2-248
2.8.123 FRCDSWTOPRI, page 2-111	2.8.235 MANUAL-REQ-RING, page 2-178	2.8.369 VCG-DEG, page 2-253
2.8.124 FRCDSWTOSEC, page 2-112	2.8.236 MANUAL-REQ-SPAN, page 2-179	2.8.370 VCG-DOWN, page 2-253

Table 2-4 ONS 15454 NA Conditions Index (continued)

2.8.125 FRCDSWTOTHIRD, page 2-112	2.8.245 NO-CONFIG, page 2-186	2.8.375 VOLT-MISM, page 2-255
2.8.126 FRNGSYNC, page 2-112	2.8.256 ODUK-SD-PM, page 2-190	2.8.376 WKSWPR, page 2-255
2.8.128 FULLPASSTHR-BI, page 2-113	2.8.257 ODUK-SF-PM, page 2-191	2.8.377 WTR, page 2-256

2.1.5 NR Conditions

Table 2-5 alphabetically lists ONS 15454 Not Reported conditions.

Table 2-5 ONS 15454 NR Conditions Index

2.8.1 AIS, page 2-30	2.8.248 ODUK-1-AIS-PM, page 2-187	2.8.266 OTUK-AIS, page 2-197
2.8.2 AIS-L, page 2-31	2.8.249 ODUK-2-AIS-PM, page 2-187	2.8.267 OTUK-BDI, page 2-197
2.8.3 AIS-P, page 2-31	2.8.250 ODUK-3-AIS-PM, page 2-188	2.8.293 RFI, page 2-212
2.8.4 AIS-V, page 2-32	2.8.251 ODUK-4-AIS-PM, page 2-188	2.8.294 RFI-L, page 2-213
2.8.30 AUTOSW-AIS, page 2-47	2.8.252 ODUK-AIS-PM, page 2-188	2.8.295 RFI-P, page 2-213
2.8.81 ERFI-P-CONN, page 2-84	2.8.253 ODUK-BDI-PM, page 2-189	2.8.296 RFI-V, page 2-214
2.8.82 ERFI-P-PAYLD, page 2-84	2.8.254 ODUK-LCK-PM, page 2-189	2.8.361 TX-AIS, page 2-247
2.8.83 ERFI-P-SRVR, page 2-85	2.8.255 ODUK-OCI-PM, page 2-190	—

2.2 Alarms and Conditions Indexed By Alphabetical Entry

Table 2-6 alphabetically lists all ONS 15454 alarms and conditions.

Table 2-6 ONS 15454 Alarm and Condition Alphabetical Index

2.8.1 AIS, page 2-30	2.8.127 FSTSYNC, page 2-113	2.8.253 ODUK-BDI-PM, page 2-189
2.8.2 AIS-L, page 2-31	2.8.128 FULLPASSTHR-BI, page 2-113	2.8.254 ODUK-LCK-PM, page 2-189
2.8.3 AIS-P, page 2-31	2.8.129 GAIN-HDEG, page 2-113	2.8.255 ODUK-OCI-PM, page 2-190
2.8.4 AIS-V, page 2-32	2.8.130 GAIN-HFAIL, page 2-115	2.8.256 ODUK-SD-PM, page 2-190
2.8.5 ALS, page 2-32	2.8.131 GAIN-LDEG, page 2-115	2.8.257 ODUK-SF-PM, page 2-191
2.8.6 AMPLI-INIT, page 2-32	2.8.132 GAIN-LFAIL, page 2-115	2.8.258 ODUK-TIM-PM, page 2-191
2.8.7 APC-CORRECTION-SKIPPED, page 2-33	2.8.133 GCC-EOC, page 2-116	2.8.259 OOU-TPT, page 2-192
2.8.8 APC-DISABLED, page 2-33	2.8.134 GE-OOSYNC, page 2-116	2.8.260 OPTNTWMIS, page 2-192
2.8.9 APC-END, page 2-34	2.8.135 GFP-CSF, page 2-117	2.8.261 OPWR-HDEG, page 2-193
2.8.10 APC-OUT-OF-RANGE, page 2-34	2.8.136 GFP-DE-MISMATCH, page 2-117	2.8.262 OPWR-HFAIL, page 2-195
2.8.11 APSB, page 2-34	2.8.137 GFP-EX-MISMATCH, page 2-118	2.8.263 OPWR-LDEG, page 2-195

Table 2-6 ONS 15454 Alarm and Condition Alphabetical Index (continued)

2.8.12 APSCDFLTK, page 2-35	2.8.138 GFP-LFD, page 2-118	2.8.264 OPWR-LFAIL, page 2-196
2.8.13 APSC-IMP, page 2-36	2.8.139 GFP-NO-BUFFERS, page 2-119	2.8.265 OSRION, page 2-196
2.8.14 APSCINCON, page 2-37	2.8.140 GFP-UP-MISMATCH, page 2-119	2.8.266 OTUK-AIS, page 2-197
2.8.15 APSCM, page 2-37	2.8.141 HELLO, page 2-120	2.8.267 OTUK-BDI, page 2-197
2.8.16 APSCNMIS, page 2-38	2.8.142 HIBATVG, page 2-120	2.8.268 OTUK-IAE, page 2-198
2.8.17 APSIMP, page 2-39	2.8.143 HI-CCVOLT, page 2-121	2.8.269 OTUK-LOF, page 2-199
2.8.18 APS-INV-PRIM, page 2-40	2.8.144 HI-LASERBIAS, page 2-121	2.8.270 OTUK-SD, page 2-199
2.8.19 APS-PRIM-FAC, page 2-40	2.8.145 HI-LASERTEMP, page 2-122	2.8.271 OTUK-SF, page 2-200
2.8.20 APSMM, page 2-40	2.8.146 HI-RXPOWER, page 2-123	2.8.272 OTUK-TIM, page 2-200
2.8.21 APS-PRIM-SEC-MISM, page 2-41	2.8.147 HITEMP, page 2-124	2.8.273 OUT-OF-SYNC, page 2-201
2.8.22 AS-CMD, page 2-42	2.8.148 HI-TXPOWER, page 2-125	2.8.274 PARAM-MISM, page 2-201
2.8.23 AS-MT, page 2-43	2.8.149 HLDOVRSYNC, page 2-125	2.8.275 PDI-P, page 2-201
2.8.24 AS-MT-OOG, page 2-43	2.8.150 I-HITEMP, page 2-126	2.8.276 PEER-NORESPONSE, page 2-203
2.8.25 AUD-LOG-LOSS, page 2-44	2.8.151 IMPROPRMVL, page 2-127	2.8.277 PLM-P, page 2-204
2.8.26 AUD-LOG-LOW, page 2-45	2.8.152 INC-ISD, page 2-128	2.8.278 PLM-V, page 2-205
2.8.27 AU-LOF, page 2-45	2.8.153 INHSWPR, page 2-128	2.8.279 PORT-ADD-PWR-DEG-HI, page 2-205
2.8.28 AUTOLSROFF, page 2-45	2.8.154 INHSWWKG, page 2-129	2.8.280 PORT-ADD-PWR-DEG-LOW, page 2-205
2.8.29 AUTORESET, page 2-46	2.8.155 INTRUSION-PSWD, page 2-129	2.8.281 PORT-ADD-PWR-FAIL-HI, page 2-205
2.8.30 AUTOSW-AIS, page 2-47	2.8.156 INVMACADR, page 2-130	2.8.282 PORT-ADD-PWR-FAIL-LOW, page 2-205
2.8.31 AUTOSW-LOP (STSMON), page 2-47	2.8.157 IOSCFGCOPY, page 2-132	2.8.283 PORT-MISMATCH, page 2-207
2.8.32 AUTOSW-LOP (VT-MON), page 2-48	2.8.158 KB-PASSTHR, page 2-132	2.8.284 PRC-DUPID, page 2-207
2.8.33 AUTOSW-PDI, page 2-48	2.8.159 KBYTE-APS-CHANNEL-FAILURE, page 2-133	2.8.285 PROTNA, page 2-208
2.8.34 AUTOSW-SDBER, page 2-49	2.8.160 LAN-POL-REV, page 2-133	2.8.286 PTIM, page 2-208
2.8.35 AUTOSW-SFBER, page 2-49	2.8.161 LASER-APR, page 2-134	2.8.287 PWR-FAIL-A, page 2-209
2.8.36 AUTOSW-UNEQ (STSMON), page 2-49	2.8.162 LASERBIAS-DEG, page 2-134	2.8.288 PWR-FAIL-B, page 2-210
2.8.37 AUTOSW-UNEQ (VT-MON), page 2-50	2.8.163 LASERBIAS-FAIL, page 2-134	2.8.289 PWR-FAIL-RET-A, page 2-210
2.8.38 AWG-DEG, page 2-50	2.8.164 LASEREOL, page 2-135	2.8.290 PWR-FAIL-RET-B, page 2-211

Table 2-6 ONS 15454 Alarm and Condition Alphabetical Index (continued)

2.8.39 AWG-FAIL, page 2-50	2.8.165 LASERTEMP-DEG, page 2-135	2.8.291 RAI, page 2-211
2.8.40 AWG-OVERTEMP, page 2-51	2.8.166 LCAS-CRC, page 2-136	2.8.292 RCVR-MISS, page 2-212
2.8.41 AWG-WARM-UP, page 2-51	2.8.167 LCAS-RX-FAIL, page 2-137	2.8.293 RFI, page 2-212
2.8.42 BAT-FAIL, page 2-51	2.8.168 LCAS-TX-ADD, page 2-137	2.8.294 RFI-L, page 2-213
2.8.43 BKUPMEMP, page 2-52	2.8.169 LCAS-TX-DNU, page 2-138	2.8.295 RFI-P, page 2-213
2.8.44 BLSROSYNC, page 2-53	2.8.170 LKOUTPR-S, page 2-138	2.8.296 RFI-V, page 2-214
2.8.45 BPV, page 2-54	2.8.171 LOA, page 2-138	2.8.297 RING-ID-MIS, page 2-215
2.8.46 CARLOSS (CE100T), page 2-54	2.8.172 LOCKOUT-REQ, page 2-139	2.8.298 RING-MISMATCH, page 2-215
2.8.47 CARLOSS (E100T, E1000F), page 2-54	2.8.173 LOF (BITS), page 2-139	2.8.299 RING-SW-EAST, page 2-216
2.8.48 CARLOSS (EQPT), page 2-56	2.8.174 LOF (DS1), page 2-140	2.8.300 RING-SW-WEST, page 2-216
2.8.49 CARLOSS (FC), page 2-58	2.8.175 LOF (DS3), page 2-141	2.8.301 RPRW, page 2-216
2.8.50 CARLOSS (G1000), page 2-58	2.8.176 LOF (EC1), page 2-142	2.8.302 RUNCFG-SAVENEED, page 2-217
2.8.51 CARLOSS (GE), page 2-61	2.8.177 LOF (OCN), page 2-143	2.8.303 SD (DS1, DS3), page 2-217
2.8.52 CARLOSS (ISC), page 2-61	2.8.178 LOF (TRUNK), page 2-143	2.8.304 SD (TRUNK), page 2-219
2.8.53 CARLOSS (ML100T, ML1000), page 2-62	2.8.179 LO-LASERTEMP, page 2-144	2.8.305 SD-L, page 2-219
2.8.54 CARLOSS (TRUNK), page 2-63	2.8.180 LOM, page 2-144	2.8.306 SD-P, page 2-220
2.8.55 CASETEMP-DEG, page 2-63	2.8.181 LOP-P, page 2-145	2.8.307 SD-V, page 2-220
2.8.56 CLDRESTART, page 2-64	2.8.182 LOP-V, page 2-145	2.8.308 SF (DS1, DS3), page 2-221
2.8.57 COMIOXC, page 2-64	2.8.183 LO-RXPOWER, page 2-146	2.8.309 SF (TRUNK), page 2-222
2.8.58 COMM-FAIL, page 2-65	2.8.184 LOS (2R), page 2-147	2.8.310 SF-L, page 2-223
2.8.59 CONTBUS-A-18, page 2-66	2.8.185 LOS (BITS), page 2-147	2.8.311 SF-P, page 2-223
2.8.60 CONTBUS-B-18, page 2-66	2.8.186 LOS (DS1), page 2-148	2.8.312 SF-V, page 2-223
2.8.61 CONTBUS-IO-A, page 2-67	2.8.187 LOS (DS3), page 2-149	2.8.313 SFTWDOWN, page 2-224
2.8.62 CONTBUS-IO-B, page 2-68	2.8.188 LOS (EC1, EC1-12), page 2-150	2.8.314 SH-INS-LOSS-VAR-DEG-HIGH, page 2-224
2.8.63 CTNEQPT-MISMATCH, page 2-69	2.8.189 LOS (ESCON), page 2-151	2.8.315 SH-INS-LOSS-VAR-DEG-LOW, page 2-225
2.8.64 CTNEQPT-PBPROT, page 2-70	2.8.190 LOS (FUDC), page 2-151	2.8.316 SHUTTER-OPEN, page 2-225
2.8.65 CTNEQPT-PBWORK, page 2-71	2.8.191 LOS (ISC), page 2-152	2.8.317 SIGLOSS, page 2-225
2.8.66 DATAFLT, page 2-73	2.8.192 LOS (MSUDC), page 2-153	2.8.318 SNTP-HOST, page 2-226
2.8.67 DBOSYNC, page 2-73	2.8.193 LOS (OCN), page 2-153	2.8.319 SPAN-SW-EAST, page 2-227
2.8.68 DS3-MISM, page 2-74	2.8.194 LOS (OTS), page 2-155	2.8.320 SPAN-SW-WEST, page 2-227
2.8.69 DSP-COMM-FAIL, page 2-75	2.8.195 LOS (TRUNK), page 2-156	2.8.321 SQUELCH, page 2-227
2.8.70 DSP-FAIL, page 2-75	2.8.196 LOS-O, page 2-157	2.8.322 SQUELCHED, page 2-229

Table 2-6 ONS 15454 Alarm and Condition Alphabetical Index (continued)

2.8.71 DUP-IPADDR, page 2-75	2.8.197 LOS-P (OCH), page 2-159	2.8.323 SQM, page 2-230
2.8.72 DUP-NODENAME, page 2-76	2.8.198 LOS-P (OMS, OTS), page 2-161	2.8.324 SSM-DUS, page 2-231
2.8.73 EHIBATVG, page 2-76	2.8.199 LOS-P (TRUNK), page 2-163	2.8.325 SSM-FAIL, page 2-231
2.8.74 ELWBATVG, page 2-77	2.8.200 LO-TXPOWER, page 2-164	2.8.326 SSM-LNC, page 2-232
2.8.75 ENCAP-MISMATCH-P, page 2-77	2.8.201 LPBKCRS, page 2-165	2.8.327 SSM-OFF, page 2-232
2.8.76 EOC, page 2-79	2.8.202 LPBKDS1FEAC, page 2-166	2.8.328 SSM-PRC, page 2-232
2.8.77 EOC-L, page 2-81	2.8.203 LPBKDS1FEAC-CMD, page 2-166	2.8.329 SSM-PRS, page 2-233
2.8.78 EQPT, page 2-82	2.8.204 LPBKDS3FEAC, page 2-166	2.8.330 SSM-RES, page 2-233
2.8.79 EQPT-DIAG, page 2-83	2.8.205 LPBKDS3FEAC-CMD, page 2-167	2.8.331 SSM-SDN-TN, page 2-233
2.8.80 EQPT-MISS, page 2-83	2.8.206 LPBKFACILITY (CE100T), page 2-167	2.8.332 SSM-SETS, page 2-233
2.8.81 ERFI-P-CONN, page 2-84	2.8.207 LPBKFACILITY (DS1, DS3), page 2-168	2.8.333 SSM-SMC, page 2-233
2.8.82 ERFI-P-PAYLD, page 2-84	2.8.208 LPBKFACILITY (EC1), page 2-168	2.8.334 SSM-ST2, page 2-234
2.8.83 ERFI-P-SRVR, page 2-85	2.8.209 LPBKFACILITY (ESCON), page 2-169	2.8.335 SSM-ST3, page 2-234
2.8.84 ERROR-CONFIG, page 2-85	2.8.210 LPBKFACILITY (FC), page 2-169	2.8.336 SSM-ST3E, page 2-234
2.8.85 ETH-LINKLOSS, page 2-86	2.8.211 LPBKFACILITY (FCMR), page 2-169	2.8.337 SSM-ST4, page 2-234
2.8.86 E-W-MISMATCH, page 2-87	2.8.212 LPBKFACILITY (G1000), page 2-169	2.8.338 SSM-STU, page 2-235
2.8.87 EXCCOL, page 2-89	2.8.213 LPBKFACILITY (GE), page 2-170	2.8.339 SSM-TNC, page 2-235
2.8.88 EXERCISE-RING-FAIL, page 2-89	2.8.214 LPBKFACILITY (ISC), page 2-170	2.8.340 SWMTXMOD, page 2-235
2.8.89 EXERCISE-SPAN-FAIL, page 2-90	2.8.215 LPBKFACILITY (OCN), page 2-171	2.8.341 SWTOPRI, page 2-237
2.8.90 EXT, page 2-90	2.8.216 LPBKFACILITY (TRUNK), page 2-171	2.8.342 SWTOSEC, page 2-237
2.8.91 EXTRA-TRAF-PREEMPT, page 2-91	2.8.217 LPKTERMINAL (CE100T), page 2-172	2.8.343 SWTOTHIRD, page 2-237
2.8.92 FAILTOSW, page 2-91	2.8.218 LPBKTERMINAL (DS1, DS3), page 2-172	2.8.344 SYNC-FREQ, page 2-238
2.8.93 FAILTOSW-PATH, page 2-92	2.8.219 LPBKTERMINAL (EC1), page 2-173	2.8.345 SYNCLOSS, page 2-238

Table 2-6 ONS 15454 Alarm and Condition Alphabetical Index (continued)

2.8.94 FAILTOSWR, page 2-93	2.8.220 LPBKTERMINAL (ESCON), page 2-173	2.8.346 SYNCPRI, page 2-239
2.8.95 FAILTOSWS, page 2-95	2.8.221 LPBKTERMINAL (FC), page 2-173	2.8.347 SYNCSEC, page 2-240
2.8.96 FAN, page 2-97	2.8.222 LPBKTERMINAL (FCMR), page 2-174	2.8.348 SYNCTHIRD, page 2-240
2.8.97 FC-NO-CREDITS, page 2-98	2.8.223 LPBKTERMINAL (G1000), page 2-174	2.8.349 SYSBOOT, page 2-241
2.8.98 FE-AIS, page 2-99	2.8.224 LPBKTERMINAL (GE), page 2-175	2.8.350 TEMP-MISM, page 2-241
2.8.99 FEC-MISM, page 2-99	2.8.225 LPBKTERMINAL (ISC), page 2-175	2.8.351 TIM, page 2-242
2.8.100 FE-DS1-MULTLOS, page 2-100	2.8.226 LPBKTERMINAL (OCN), page 2-175	2.8.352 TIM-MON, page 2-243
2.8.101 FE-DS1-NSA, page 2-100	2.8.227 LPBKTERMINAL (TRUNK), page 2-176	2.8.353 TIM-P, page 2-243
2.8.102 FE-DS1-SA, page 2-101	2.8.228 LWBATVG, page 2-176	2.8.354 TIM-V, page 2-244
2.8.103 FE-DS1-SNGLLOS, page 2-101	2.8.229 MAN-REQ, page 2-177	2.8.355 TPTFAIL (CE100T), page 2-244
2.8.104 FE-DS3-NSA, page 2-102	2.8.230 MANRESET, page 2-177	2.8.356 TPTFAIL (FCMR), page 2-244
2.8.105 FE-DS3-SA, page 2-102	2.8.231 MANSWTOINT, page 2-177	2.8.357 TPTFAIL (G1000), page 2-245
2.8.106 FE-EQPT-NSA, page 2-103	2.8.232 MANSWTOPRI, page 2-178	2.8.358 TPTFAIL (ML100T, ML1000), page 2-245
2.8.107 FE-FRCDWKSWBK-SPAN, page 2-104	2.8.233 MANSWTOSEC, page 2-178	2.8.359 TRMT, page 2-246
2.8.108 FE-FRCDWKSWPR-RING, page 2-104	2.8.234 MANSWTO THIRD, page 2-178	2.8.360 TRMT-MISS, page 2-247
2.8.109 FE-FRCDWKSWPR-SPAN, page 2-105	2.8.235 MANUAL-REQ-RING, page 2-178	2.8.361 TX-AIS, page 2-247
2.8.110 FE-IDLE, page 2-105	2.8.236 MANUAL-REQ-SPAN, page 2-179	2.8.362 TX-RAI, page 2-248
2.8.111 FE-LOCKOUTOFPR-SPAN, page 2-106	2.8.237 MEA (AIP), page 2-179	2.8.363 UNC-WORD, page 2-248
2.8.112 FE-LOF, page 2-106	2.8.238 MEA (BIC), page 2-179	2.8.364 UNEQ-P, page 2-249
2.8.113 FE-LOS, page 2-107	2.8.239 MEA (EQPT), page 2-181	2.8.365 UNEQ-V, page 2-251
2.8.114 FE-MANWKSWBK-SPAN, page 2-107	2.8.240 MEA (FAN), page 2-183	2.8.366 UNREACHABLE-TARGET-POWER, page 2-251
2.8.115 FE-MANWKSWPR-RING, page 2-108	2.8.241 MEA (PPM), page 2-183	2.8.367 UT-COMM-FAIL, page 2-252
2.8.116 FE-MANWKSWPR-SPAN, page 2-109	2.8.242 MEM-GONE, page 2-184	2.8.368 UT-FAIL, page 2-252
2.8.117 FEPRLF, page 2-109	2.8.243 MEM-LOW, page 2-184	2.8.369 VCG-DEG, page 2-253

Table 2-6 ONS 15454 Alarm and Condition Alphabetical Index (continued)

2.8.118 FIBERTEMP-DEG, page 2-110	2.8.244 MFGMEM, page 2-185	2.8.370 VCG-DOWN, page 2-253
2.8.119 FORCED-REQ, page 2-110	2.8.245 NO-CONFIG, page 2-186	2.8.371 VOA-HDEG, page 2-253
2.8.120 FORCED-REQ-RING, page 2-110	2.8.246 NOT-AUTHENTICATED, page 2-186	2.8.372 VOA-HFAIL, page 2-254
2.8.121 FORCED-REQ-SPAN, page 2-111	2.8.247 OCHNC-INC, page 2-187	2.8.373 VOA-LDEG, page 2-254
2.8.122 FRCDSWTOINT, page 2-111	2.8.248 ODUK-1-AIS-PM, page 2-187	2.8.374 VOA-LFAIL, page 2-255
2.8.123 FRCDSWTOPRI, page 2-111	2.8.249 ODUK-2-AIS-PM, page 2-187	2.8.375 VOLT-MISM, page 2-255
2.8.124 FRCDSWTOSEC, page 2-112	2.8.250 ODUK-3-AIS-PM, page 2-188	2.8.376 WKSWPR, page 2-255
2.8.125 FRCDSWTOTHIRD, page 2-112	2.8.251 ODUK-4-AIS-PM, page 2-188	2.8.377 WTR, page 2-256
2.8.126 FRNGSYNC, page 2-112	2.8.252 ODUK-AIS-PM, page 2-188	2.8.378 WVL-MISMATCH, page 2-256

2.3 Alarm Logical Objects

The CTC alarm profile list organizes all alarms and conditions according to the logical objects they are raised against. These logical objects represent physical objects such as cards, logical objects such as circuits, or transport and signal monitoring entities such as the SONET or ITU-T G.709 optical overhead bits. One alarm might appear in multiple entries when it can be raised against multiple objects. For example, the loss of signal (LOS) alarm can be raised against the optical signal (OC-N) or the optical transport layer overhead (OTN) as well as other objects. Therefore, both OCN:LOS and OTN:LOS appear in the list (as well as the other objects).

Alarm profile list objects are defined in [Table 2-7](#).



Note

Alarm logical object names can appear as abbreviated versions of standard terms used in the system and the documentation. For example, the “OCN” logical object refers to the OC-N signal. Logical object names or industry-standard terms are used within the entries as appropriate.

Table 2-7 Alarm Logical Object Type Definition

Logical Object	Definition
2R	Reshape and retransmit (used for transponder [TXP] cards).
AICI-AEP	Alarm Interface Controller–International/alarm expansion panel. A combination term that refers to this platform’s AIC card.
AIP	Auxiliary interface protection module.
AOTS	Amplified optical transport section.
BIC	Backplane interface connector.
BITS	Building integrated timing supply incoming references (BITS-1, BITS-2).

Table 2-7 Alarm Logical Object Type Definition (continued)

Logical Object	Definition
BPLANE	The backplane.
CE100T	CE-100T-8 card.
DS1	A DS-1 line on a DS-1 or DS-3 electrical card (DS1-14, DS1N-14, DS3N-12E, DS3XM-6, DS3XM-12).
DS3	A DS-3 line on a DS-3 electrical card (DS3-12, DS3N-12, DS3-12E, DS3XM-6, and DS3XM-12).
E1000F	An E1000 Ethernet card (E1000-2, E1000-2G).
E100T	An E100 Ethernet card (E100T-12, E100T-G).
EC1	Any EC1 port (including EC1-12 card ports).
EC1-12	An EC1-12 electrical card.
ENVALRM	An environmental alarm port.
EQPT	A card, its physical objects, and its logical objects as they are located in any of the eight non-common card slots. The EQPT object is used for alarms that refer to the card itself and all other objects on the card including ports, lines, synchronous transport signals (STS), and virtual tributaries (VT).
ESCON	Enterprise System Connection fiber optic technology, referring to the following TXP cards: TXP_MR_2.5G, TXPP_MR_2.5G.
EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2).
FAN	Fan-tray assembly.
FC	Fibre channel data transfer architecture, referring to the following muxponder (MXP) or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E.
FCMR	An FC_MR-4 Fibre Channel card.
FUDC	SONET F1 byte user data channel for ONS 15454 ML-Series Ethernet cards.
G1000	A G1000 Ethernet card (G1000-4).
GE	Gigabit Ethernet, referring to the following MXP or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10G.
GFP-FAC	Generic framing procedure facility port, referring to all MXP and TXP cards.
ISC	Inter-service channel, referring to MXP and TXP cards.
ML1000	An ML1000 Ethernet card (ML1000-2).
ML100T	An ML100 card (ML100T-12).
MSUDC	Multiplex section user data channel.
NE	The entire network element.
NE-SREF	The timing status of the NE.
OCH	The optical channel, referring to dense wavelength division multiplexing (DWDM) cards.
OCHNC-CONN	The optical channel connection, referring to DWDM cards.
OCN	An OC-N line on any OC-N card.

Table 2-7 Alarm Logical Object Type Definition (continued)

Logical Object	Definition
OMS	Optical multiplex section.
OSC-RING	Optical service channel ring.
OTS	Optical transport section.
PPM	Pluggable port module, referring to MXP and TXP cards.
PWR	Power equipment.
STSMON	STS alarm detection at the monitor point (upstream from the cross-connect).
STSTRM	STS alarm detection at termination (downstream from the cross-connect).
TRUNK	The optical or DWDM card carrying the high-speed signal; referring to MXP or TXP cards.
VCG	A virtual concatenation group of VTs.
VT-MON	VT1 alarm detection at the monitor point (upstream from the cross-connect).
VT-TERM	VT1 alarm detection at termination (downstream from the cross-connect).

2.4 Alarm Index by Logical Object Type

Table 2-8 lists all ONS 15454 Release 5.0 alarms and logical objects as they are given in the system alarm profile. The list entries are organized by logical object name and then by alarm or condition name. Each entry contains a page number that refers to an alarm description in this chapter. Where appropriate, the alarm entries also contain troubleshooting procedures.


Note

In a mixed network containing different types of nodes (such as ONS 15310, ONS 15454, and ONS 15600), the initially displayed alarm list in the Provisioning > Alarm Profiles > Alarm Profile Editor tab lists all conditions applicable to all nodes in the network. However, when you load the default severity profile from a node, only applicable alarms will display severity levels. Nonapplicable alarms can display “use default” or “unset.”


Note

In some cases this list does not follow alphabetical order, but it does reflect the order shown in CTC.

Table 2-8 Alarm Index by Logical Object

2R: 2.8.5 ALS, page 2-32	FC: 2.8.172 LOCKOUT-REQ, page 2-139	OCN: 2.8.310 SF-L, page 2-223
2R: 2.8.22 AS-CMD, page 2-42	FC: 2.8.210 LPBKFACILITY (FC), page 2-169	OCN: 2.8.319 SPAN-SW-EAST, page 2-227
2R: 2.8.23 AS-MT, page 2-43	FC: 2.8.221 LPBKTERMINAL (FC), page 2-173	OCN: 2.8.320 SPAN-SW-WEST, page 2-227
2R: 2.8.92 FAILTOSW, page 2-91	FC: 2.8.236 MANUAL-REQ-SPAN, page 2-179	OCN: 2.8.321 SQUELCH, page 2-227

Table 2-8 Alarm Index by Logical Object (continued)

2R: 2.8.121 FORCED-REQ-SPAN, page 2-111	FC: 2.8.273 OUT-OF-SYNC, page 2-201	OCN: 2.8.322 SQUELCHED, page 2-229
2R: 2.8.144 HI-LASERBIAS, page 2-121	FC: 2.8.317 SIGLOSS, page 2-225	OCN: 2.8.324 SSM-DUS, page 2-231
2R: 2.8.146 HI-RXPOWER, page 2-123	FC: 2.8.322 SQUELCHED, page 2-229	OCN: 2.8.325 SSM-FAIL, page 2-231
2R: 2.8.148 HI-TXPOWER, page 2-125	FC: 2.8.345 SYNCLOSS, page 2-238	OCN: 2.8.327 SSM-OFF, page 2-232
2R: 2.8.183 LO-RXPOWER, page 2-146	FC: 2.8.376 WKSWPR, page 2-255	OCN: 2.8.329 SSM-PRS, page 2-233
2R: 2.8.200 LO-TXPOWER, page 2-164	FC: 2.8.377 WTR, page 2-256	OCN: 2.8.330 SSM-RES, page 2-233
2R: 2.8.172 LOCKOUT-REQ, page 2-139	FCMR: 2.8.22 AS-CMD, page 2-42	OCN: 2.8.333 SSM-SMC, page 2-233
2R: 2.8.184 LOS (2R), page 2-147	FCMR: 2.8.23 AS-MT, page 2-43	OCN: 2.8.334 SSM-ST2, page 2-234
2R: 2.8.236 MANUAL-REQ-SPAN, page 2-179	FCMR: 2.8.97 FC-NO-CREDITS, page 2-98	OCN: 2.8.335 SSM-ST3, page 2-234
2R: 2.8.322 SQUELCHED, page 2-229	FCMR: 2.8.135 GFP-CSF, page 2-117	OCN: 2.8.336 SSM-ST3E, page 2-234
2R: 2.8.376 WKSWPR, page 2-255	FCMR: 2.8.136 GFP-DE-MISMATCH, page 2-117	OCN: 2.8.337 SSM-ST4, page 2-234
2R: 2.8.377 WTR, page 2-256	FCMR: 2.8.137 GFP-EX-MISMATCH, page 2-118	OCN: 2.8.338 SSM-STU, page 2-235
AICI-AEP: 2.8.78 EQPT, page 2-82	FCMR: 2.8.138 GFP-LFD, page 2-118	OCN: 2.8.339 SSM-TNC, page 2-235
AICI-AEP: 2.8.244 MFGMEM, page 2-185	FCMR: 2.8.139 GFP-NO-BUFFERS, page 2-119	OCN: 2.8.344 SYNC-FREQ, page 2-238
AICI-AIE: 2.8.78 EQPT, page 2-82	FCMR: 2.8.140 GFP-UP-MISMATCH, page 2-119	OCN: 2.8.351 TIM, page 2-242
AICI-AIE: 2.8.244 MFGMEM, page 2-185	FCMR: 2.8.211 LPBKFACILITY (FCMR), page 2-169	OCN: 2.8.352 TIM-MON, page 2-243
AIP: 2.8.156 INVMACADR, page 2-130	FCMR: 2.8.222 LPBKTERMINAL (FCMR), page 2-174	OCN: 2.8.376 WKSWPR, page 2-255
AIP: 2.8.237 MEA (AIP), page 2-179	FCMR: 2.8.283 PORT-MISMATCH, page 2-207	OCN: 2.8.377 WTR, page 2-256
AIP: 2.8.244 MFGMEM, page 2-185	FCMR: 2.8.317 SIGLOSS, page 2-225	OMS: 2.8.7 APC-CORRECTION-SKIPPED, page 2-33
AOTS: 2.8.5 ALS, page 2-32	FCMR: 2.8.345 SYNCLOSS, page 2-238	OMS: 2.8.10 APC-OUT-OF-RANGE, page 2-34
AOTS: 2.8.6 AMPLI-INIT, page 2-32	FCMR: 2.8.356 TPTFAIL (FCMR), page 2-244	OMS: 2.8.22 AS-CMD, page 2-42

Table 2-8 Alarm Index by Logical Object (continued)

AOTS: 2.8.7 APC-CORRECTION-SKIPPE D, page 2-33	FUDC: 2.8.1 AIS, page 2-30	OMS: 2.8.23 AS-MT, page 2-43
AOTS: 2.8.10 APC-OUT-OF-RANGE, page 2-34	FUDC: 2.8.190 LOS (FUDC), page 2-151	OMS: 2.8.196 LOS-O, page 2-157
AOTS: 2.8.22 AS-CMD, page 2-42	G1000: 2.8.22 AS-CMD, page 2-42	OMS: 2.8.198 LOS-P (OMS, OTS), page 2-161
AOTS: 2.8.23 AS-MT, page 2-43	G1000: 2.8.23 AS-MT, page 2-43	OMS: 2.8.261 OPWR-HDEG, page 2-193
AOTS: 2.8.55 CASTEMP-DEG, page 2-63	G1000: 2.8.50 CARLOSS (G1000), page 2-58	OMS: 2.8.262 OPWR-HFAIL, page 2-195
AOTS: 2.8.118 FIBERTEMP-DEG, page 2-110	G1000: 2.8.212 LPBKFACILITY (G1000), page 2-169	OMS: 2.8.263 OPWR-LDEG, page 2-195
AOTS: 2.8.129 GAIN-HDEG, page 2-113	G1000: 2.8.223 LPBKTERMINAL (G1000), page 2-174	OMS: 2.8.264 OPWR-LFAIL, page 2-196
AOTS: 2.8.130 GAIN-HFAIL, page 2-115	G1000: 2.8.357 TPTFAIL (G1000), page 2-245	OMS: 2.8.274 PARAM-MISM, page 2-201
AOTS: 2.8.131 GAIN-LDEG, page 2-115	GE: 2.8.5 ALS, page 2-32	OMS: 2.8.371 VOA-HDEG, page 2-253
AOTS: 2.8.132 GAIN-LFAIL, page 2-115	GE: 2.8.22 AS-CMD, page 2-42	OMS: 2.8.372 VOA-HFAIL, page 2-254
AOTS: 2.8.161 LASER-APR, page 2-134	GE: 2.8.23 AS-MT, page 2-43	OMS: 2.8.373 VOA-LDEG, page 2-254
AOTS: 2.8.162 LASERBIAS-DEG, page 2-134	GE: 2.8.51 CARLOSS (GE), page 2-61	OMS: 2.8.374 VOA-LFAIL, page 2-255
AOTS: 2.8.163 LASERBIAS-FAIL, page 2-134	GE: 2.8.92 FAILTOSW, page 2-91	OSC-RING: 2.8.297 RING-ID-MIS, page 2-215
AOTS: 2.8.165 LASERTEMP-DEG, page 2-135	GE: 2.8.121 FORCED-REQ-SPAN, page 2-111	OTS: 2.8.7 APC-CORRECTION-SKIPPED, page 2-33
AOTS: 2.8.261 OPWR-HDEG, page 2-193	GE: 2.8.134 GE-OOSYNC, page 2-116	OTS: 2.8.10 APC-OUT-OF-RANGE, page 2-34
AOTS: 2.8.262 OPWR-HFAIL, page 2-195	GE: 2.8.144 HI-LASERBIAS, page 2-121	OTS: 2.8.22 AS-CMD, page 2-42
AOTS: 2.8.263 OPWR-LDEG, page 2-195	GE: 2.8.146 HI-RXPOWER, page 2-123	OTS: 2.8.23 AS-MT, page 2-43
AOTS: 2.8.264 OPWR-LFAIL, page 2-196	GE: 2.8.148 HI-TXPOWER, page 2-125	OTS: 2.8.38 AWG-DEG, page 2-50
AOTS: 2.8.265 OSRION, page 2-196	GE: 2.8.183 LO-RXPOWER, page 2-146	OTS: 2.8.39 AWG-FAIL, page 2-50
AOTS: 2.8.274 PARAM-MISM, page 2-201	GE: 2.8.200 LO-TXPOWER, page 2-164	OTS: 2.8.40 AWG-OVERTEMP, page 2-51

Table 2-8 Alarm Index by Logical Object (continued)

AOTS: 2.8.371 VOA-HDEG, page 2-253	GE: 2.8.172 LOCKOUT-REQ, page 2-139	OTS: 2.8.41 AWG-WARM-UP, page 2-51
AOTS: 2.8.372 VOA-HFAIL, page 2-254	GE: 2.8.213 LPBKFACILITY (GE), page 2-170	OTS: 2.8.162 LASERBIAS-DEG, page 2-134
AOTS: 2.8.373 VOA-LDEG, page 2-254	GE: 2.8.224 LPBKTERMINAL (GE), page 2-175	OTS: 2.8.194 LOS (OTS), page 2-155
AOTS: 2.8.374 VOA-LFAIL, page 2-255	GE: 2.8.236 MANUAL-REQ-SPAN, page 2-179	OTS: 2.8.196 LOS-O, page 2-157
BIC: 2.8.238 MEA (BIC), page 2-179	GE: 2.8.273 OUT-OF-SYNC, page 2-201	OTS: 2.8.198 LOS-P (OMS, OTS), page 2-161
BITS: 2.8.1 AIS, page 2-30	GE: 2.8.317 SIGLOSS, page 2-225	OTS: 2.8.261 OPWR-HDEG, page 2-193
BITS: 2.8.45 BPV, page 2-54	GE: 2.8.322 SQUELCHED, page 2-229	OTS: 2.8.262 OPWR-HFAIL, page 2-195
BITS: 2.8.143 HI-CCVOLT, page 2-121	GE: 2.8.345 SYNCLOSS, page 2-238	OTS: 2.8.263 OPWR-LDEG, page 2-195
BITS: 2.8.173 LOF (BITS), page 2-139	GE: 2.8.376 WKSWPR, page 2-255	OTS: 2.8.264 OPWR-LFAIL, page 2-196
BITS: 2.8.185 LOS (BITS), page 2-147	GE: 2.8.377 WTR, page 2-256	OTS: 2.8.265 OSRION, page 2-196
BITS: 2.8.324 SSM-DUS, page 2-231	GFP-FAC: 2.8.22 AS-CMD, page 2-42	OTS: 2.8.274 PARAM-MISM, page 2-201
BITS: 2.8.325 SSM-FAIL, page 2-231	GFP-FAC: 2.8.23 AS-MT, page 2-43	OTS: 2.8.314 SH-INS-LOSS-VAR-DEG-HIGH, page 2-224
BITS: 2.8.327 SSM-OFF, page 2-232	GFP-FAC: 2.8.135 GFP-CSF, page 2-117	OTS: 2.8.315 SH-INS-LOSS-VAR-DEG-LOW, page 2-225
BITS: 2.8.329 SSM-PRS, page 2-233	GFP-FAC: 2.8.136 GFP-DE-MISMATCH, page 2-117	OTS: 2.8.316 SHUTTER-OPEN, page 2-225
BITS: 2.8.330 SSM-RES, page 2-233	GFP-FAC: 2.8.137 GFP-EX-MISMATCH, page 2-118	OTS: 2.8.371 VOA-HDEG, page 2-253
BITS: 2.8.333 SSM-SMC, page 2-233	GFP-FAC: 2.8.138 GFP-LFD, page 2-118	OTS: 2.8.372 VOA-HFAIL, page 2-254
BITS: 2.8.334 SSM-ST2, page 2-234	GFP-FAC: 2.8.139 GFP-NO-BUFFERS, page 2-119	OTS: 2.8.373 VOA-LDEG, page 2-254
BITS: 2.8.335 SSM-ST3, page 2-234	GFP-FAC: 2.8.140 GFP-UP-MISMATCH, page 2-119	OTS: 2.8.374 VOA-LFAIL, page 2-255
BITS: 2.8.336 SSM-ST3E, page 2-234	ISC: 2.8.5 ALS, page 2-32	PPM: 2.8.22 AS-CMD, page 2-42
BITS: 2.8.337 SSM-ST4, page 2-234	ISC: 2.8.22 AS-CMD, page 2-42	PPM: 2.8.23 AS-MT, page 2-43

Table 2-8 Alarm Index by Logical Object (continued)

BITS: 2.8.338 SSM-STU, page 2-235	ISC: 2.8.23 AS-MT, page 2-43	PPM: 2.8.78 EQPT, page 2-82
BITS: 2.8.339 SSM-TNC, page 2-235	ISC: 2.8.52 CARLOSS (ISC), page 2-61	PPM: 2.8.144 HI-LASERBIAS, page 2-121
BITS: 2.8.344 SYNC-FREQ, page 2-238	ISC: 2.8.92 FAILTOSW, page 2-91	PPM: 2.8.145 HI-LASERTEMP, page 2-122
BPLANE: 2.8.22 AS-CMD, page 2-42	ISC: 2.8.121 FORCED-REQ-SPAN, page 2-111	PPM: 2.8.148 HI-TXPOWER, page 2-125
BPLANE: 2.8.244 MFGMEM, page 2-185	ISC: 2.8.134 GE-OOSYNC, page 2-116	PPM: 2.8.151 IMPROPRMVL, page 2-127
CE100T: 2.8.22 AS-CMD, page 2-42	ISC: 2.8.144 HI-LASERBIAS, page 2-121	PPM: 2.8.200 LO-TXPOWER, page 2-164
CE100T: 2.8.23 AS-MT, page 2-43	ISC: 2.8.146 HI-RXPOWER, page 2-123	PPM: 2.8.241 MEA (PPM), page 2-183
CE100T: 2.8.46 CARLOSS (CE100T), page 2-54	ISC: 2.8.148 HI-TXPOWER, page 2-125	PPM: 2.8.244 MFGMEM, page 2-185
CE100T: 2.8.135 GFP-CSF, page 2-117	ISC: 2.8.183 LO-RXPOWER, page 2-146	PWR: 2.8.22 AS-CMD, page 2-42
CE100T: 2.8.138 GFP-LFD, page 2-118	ISC: 2.8.200 LO-TXPOWER, page 2-164	PWR: 2.8.42 BAT-FAIL, page 2-51
CE100T: 2.8.206 LPBKFACILITY (CE100T), page 2-167	ISC: 2.8.172 LOCKOUT-REQ, page 2-139	PWR: 2.8.73 EHIBATVG, page 2-76
CE100T: 2.8.217 LPKTERMINAL (CE100T), page 2-172	ISC: 2.8.191 LOS (ISC), page 2-152	PWR: 2.8.74 ELWBATVG, page 2-77
CE100T: 2.8.301 RPRW, page 2-216	ISC: 2.8.214 LPBKFACILITY (ISC), page 2-170	PWR: 2.8.142 HIBATVG, page 2-120
CE100T: 2.8.355 TPTFAIL (CE100T), page 2-244	ISC: 2.8.225 LPBKTERMINAL (ISC), page 2-175	PWR: 2.8.228 LWBATVG, page 2-176
DS1: 2.8.1 AIS, page 2-30	ISC: 2.8.236 MANUAL-REQ-SPAN, page 2-179	PWR: 2.8.375 VOLT-MISM, page 2-255
DS1: 2.8.22 AS-CMD, page 2-42	ISC: 2.8.273 OUT-OF-SYNC, page 2-201	STSMON: 2.8.3 AIS-P, page 2-31
DS1: 2.8.23 AS-MT, page 2-43	ISC: 2.8.317 SIGLOSS, page 2-225	STSMON: 2.8.30 AUTOSW-AIS, page 2-47
DS1: 2.8.174 LOF (DS1), page 2-140	ISC: 2.8.322 SQUELCHED, page 2-229	STSMON: 2.8.31 AUTOSW-LOP (STSMON), page 2-47
DS1: 2.8.186 LOS (DS1), page 2-148	ISC: 2.8.345 SYNCLOSS, page 2-238	STSMON: 2.8.33 AUTOSW-PDI, page 2-48
DS1: 2.8.202 LPBKDS1FEAC, page 2-166	ISC: 2.8.376 WKSWPR, page 2-255	STSMON: 2.8.34 AUTOSW-SDBER, page 2-49
DS1: 2.8.203 LPBKDS1FEAC-CMD, page 2-166	ISC: 2.8.377 WTR, page 2-256	STSMON: 2.8.35 AUTOSW-SFBER, page 2-49

Table 2-8 Alarm Index by Logical Object (continued)

DS1: 2.8.207 LPBKFACILITY (DS1, DS3), page 2-168	ML1000: 2.8.22 AS-CMD, page 2-42	STSMON: 2.8.36 AUTOSW-UNEQ (STSMON), page 2-49
DS1: 2.8.218 LPBKTERMINAL (DS1, DS3), page 2-172	ML1000: 2.8.23 AS-MT, page 2-43	STSMON: 2.8.81 ERFI-P-CONN, page 2-84
DS1: 2.8.291 RAI, page 2-211	ML1000: 2.8.53 CARLOSS (ML100T, ML1000), page 2-62	STSMON: 2.8.82 ERFI-P-PAYLD, page 2-84
DS1: 2.8.292 RCVR-MISS, page 2-212	ML1000: 2.8.135 GFP-CSF, page 2-117	STSMON: 2.8.83 ERFI-P-SRVR, page 2-85
DS1: 2.8.303 SD (DS1, DS3), page 2-217	ML1000: 2.8.136 GFP-DE-MISMATCH, page 2-117	STSMON: 2.8.93 FAILTOSW-PATH, page 2-92
DS1: 2.8.308 SF (DS1, DS3), page 2-221	ML1000: 2.8.137 GFP-EX-MISMATCH, page 2-118	STSMON: 2.8.119 FORCED-REQ, page 2-110
DS1: 2.8.359 TRMT, page 2-246	ML1000: 2.8.138 GFP-LFD, page 2-118	STSMON: 2.8.172 LOCKOUT-REQ, page 2-139
DS1: 2.8.360 TRMT-MISS, page 2-247	ML1000: 2.8.139 GFP-NO-BUFFERS, page 2-119	STSMON: 2.8.181 LOP-P, page 2-145
DS1: 2.8.361 TX-AIS, page 2-247	ML1000: 2.8.140 GFP-UP-MISMATCH, page 2-119	STSMON: 2.8.201 LPBKCRS, page 2-165
DS1: 2.8.362 TX-RAI, page 2-248	ML1000: 2.8.301 RPRW, page 2-216	STSMON: 2.8.229 MAN-REQ, page 2-177
DS3: 2.8.1 AIS, page 2-30	ML1000: 2.8.358 TPTFAIL (ML100T, ML1000), page 2-245	STSMON: 2.8.275 PDI-P, page 2-201
DS3: 2.8.22 AS-CMD, page 2-42	ML100T: 2.8.22 AS-CMD, page 2-42	STSMON: 2.8.277 PLM-P, page 2-204
DS3: 2.8.23 AS-MT, page 2-43	ML100T: 2.8.23 AS-MT, page 2-43	STSMON: 2.8.295 RFI-P, page 2-213
DS3: 2.8.68 DS3-MISM, page 2-74	ML100T: 2.8.53 CARLOSS (ML100T, ML1000), page 2-62	STSMON: 2.8.306 SD-P, page 2-220
DS3: 2.8.98 FE-AIS, page 2-99	ML100T: 2.8.135 GFP-CSF, page 2-117	STSMON: 2.8.311 SF-P, page 2-223
DS3: 2.8.100 FE-DS1-MULTLOS, page 2-100	ML100T: 2.8.136 GFP-DE-MISMATCH, page 2-117	STSMON: 2.8.353 TIM-P, page 2-243
DS3: 2.8.101 FE-DS1-NSA, page 2-100	ML100T: 2.8.137 GFP-EX-MISMATCH, page 2-118	STSMON: 2.8.364 UNEQ-P, page 2-249
DS3: 2.8.102 FE-DS1-SA, page 2-101	ML100T: 2.8.138 GFP-LFD, page 2-118	STSMON: 2.8.376 WKSWPR, page 2-255
DS3: 2.8.103 FE-DS1-SNGLLOS, page 2-101	ML100T: 2.8.139 GFP-NO-BUFFERS, page 2-119	STSMON: 2.8.377 WTR, page 2-256
DS3: 2.8.104 FE-DS3-NSA, page 2-102	ML100T: 2.8.140 GFP-UP-MISMATCH, page 2-119	STSTRM: 2.8.3 AIS-P, page 2-31

Table 2-8 Alarm Index by Logical Object (continued)

DS3: 2.8.105 FE-DS3-SA, page 2-102	ML100T: 2.8.301 RPRW, page 2-216	STSTRM: 2.8.24 AS-MT-OOG, page 2-43
DS3: 2.8.106 FE-EQPT-NSA, page 2-103	ML100T: 2.8.358 TPTFAIL (ML100T, ML1000), page 2-245	STSTRM: 2.8.27 AU-LOF, page 2-45
DS3: 2.8.110 FE-IDLE, page 2-105	MSUDC: 2.8.1 AIS, page 2-30	STSTRM: 2.8.75 ENCAP-MISMATCH-P, page 2-77
DS3: 2.8.112 FE-LOF, page 2-106	MSUDC: 2.8.192 LOS (MSUDC), page 2-153	STSTRM: 2.8.81 ERFI-P-CONN, page 2-84
DS3: 2.8.113 FE-LOS, page 2-107	NE-SREF: 2.8.122 FRCDSWTOINT, page 2-111	STSTRM: 2.8.82 ERFI-P-PAYLD, page 2-84
DS3: 2.8.152 INC-ISD, page 2-128	NE-SREF: 2.8.123 FRCDSWTOPRI, page 2-111	STSTRM: 2.8.83 ERFI-P-SRVR, page 2-85
DS3: 2.8.175 LOF (DS3), page 2-141	NE-SREF: 2.8.124 FRCDSWTOSEC, page 2-112	STSTRM: 2.8.166 LCAS-CRC, page 2-136
DS3: 2.8.187 LOS (DS3), page 2-149	NE-SREF: 2.8.125 FRCDSWTOTHIRD, page 2-112	STSTRM: 2.8.167 LCAS-RX-FAIL, page 2-137
DS3: 2.8.202 LPBKDS1FEAC, page 2-166	NE-SREF: 2.8.126 FRNGSYNC, page 2-112	STSTRM: 2.8.168 LCAS-TX-ADD, page 2-137
DS3: 2.8.204 LPBKDS3FEAC, page 2-166	NE-SREF: 2.8.127 FSTSYNC, page 2-113	STSTRM: 2.8.169 LCAS-TX-DNU, page 2-138
DS3: 2.8.205 LPBKDS3FEAC-CMD, page 2-167	NE-SREF: 2.8.149 HLDVRSYNC, page 2-125	STSTRM: 2.8.180 LOM, page 2-144
DS3: 2.8.207 LPBKFACILITY (DS1, DS3), page 2-168	NE-SREF: 2.8.231 MANSWTOINT, page 2-177	STSTRM: 2.8.181 LOP-P, page 2-145
DS3: 2.8.218 LPBKTERMINAL (DS1, DS3), page 2-172	NE-SREF: 2.8.232 MANSWTOPRI, page 2-178	STSTRM: 2.8.259 OOU-TPT, page 2-192
DS3: 2.8.291 RAI, page 2-211	NE-SREF: 2.8.233 MANSWTOSEC, page 2-178	STSTRM: 2.8.275 PDI-P, page 2-201
DS3: 2.8.303 SD (DS1, DS3), page 2-217	NE-SREF: 2.8.234 MANSWTOTHIRD, page 2-178	STSTRM: 2.8.277 PLM-P, page 2-204
DS3: 2.8.308 SF (DS1, DS3), page 2-221	NE-SREF: 2.8.329 SSM-PRS, page 2-233	STSTRM: 2.8.295 RFI-P, page 2-213
DS3: 2.8.361 TX-AIS, page 2-247	NE-SREF: 2.8.330 SSM-RES, page 2-233	STSTRM: 2.8.306 SD-P, page 2-220
DS3: 2.8.362 TX-RAI, page 2-248	NE-SREF: 2.8.333 SSM-SMC, page 2-233	STSTRM: 2.8.311 SF-P, page 2-223
E1000F: 2.8.22 AS-CMD, page 2-42	NE-SREF: 2.8.334 SSM-ST2, page 2-234	STSTRM: 2.8.323 SQM, page 2-230
E1000F: 2.8.47 CARLOSS (E100T, E1000F), page 2-54	NE-SREF: 2.8.335 SSM-ST3, page 2-234	STSTRM: 2.8.353 TIM-P, page 2-243

Table 2-8 Alarm Index by Logical Object (continued)

E100T: 2.8.22 AS-CMD, page 2-42	NE-SREF: 2.8.336 SSM-ST3E, page 2-234	STSTRM: 2.8.364 UNEQ-P, page 2-249
E100T: 2.8.47 CARLOSS (E100T, E1000F), page 2-54	NE-SREF: 2.8.337 SSM-ST4, page 2-234	TRUNK: 2.8.1 AIS, page 2-30
EC1-12: 2.8.2 AIS-L, page 2-31	NE-SREF: 2.8.338 SSM-STU, page 2-235	TRUNK: 2.8.5 ALS, page 2-32
EC1-12: 2.8.22 AS-CMD, page 2-42	NE-SREF: 2.8.339 SSM-TNC, page 2-235	TRUNK: 2.8.22 AS-CMD, page 2-42
EC1-12: 2.8.23 AS-MT, page 2-43	NE-SREF: 2.8.341 SWTOPRI, page 2-237	TRUNK: 2.8.23 AS-MT, page 2-43
EC1-12: 2.8.176 LOF (EC1), page 2-142	NE-SREF: 2.8.342 SWTOSEC, page 2-237	TRUNK: 2.8.54 CARLOSS (TRUNK), page 2-63
EC1-12: 2.8.188 LOS (EC1, EC1-12), page 2-150	NE-SREF: 2.8.343 SWTOTHIRD, page 2-237	TRUNK: 2.8.69 DSP-COMM-FAIL, page 2-75
EC1-12: 2.8.208 LPBKFACILITY (EC1), page 2-168	NE-SREF: 2.8.346 SYNCPRI, page 2-239	TRUNK: 2.8.70 DSP-FAIL, page 2-75
EC1-12: 2.8.219 LPBKTERMINAL (EC1), page 2-173	NE-SREF: 2.8.347 SYNCSEC, page 2-240	TRUNK: 2.8.76 EOC, page 2-79
EC1-12: 2.8.294 RFI-L, page 2-213	NE-SREF: 2.8.348 SYNCTHIRD, page 2-240	TRUNK: 2.8.77 EOC-L, page 2-81
EC1-12: 2.8.305 SD-L, page 2-219	NE: 2.8.8 APC-DISABLED, page 2-33	TRUNK: 2.8.92 FAILTOSW, page 2-91
EC1-12: 2.8.310 SF-L, page 2-223	NE: 2.8.9 APC-END, page 2-34	TRUNK: 2.8.99 FEC-MISM, page 2-99
EC1: 2.8.2 AIS-L, page 2-31	NE: 2.8.22 AS-CMD, page 2-42	TRUNK: 2.8.121 FORCED-REQ-SPAN, page 2-111
EC1: 2.8.22 AS-CMD, page 2-42	NE: 2.8.25 AUD-LOG-LOSS, page 2-44	TRUNK: 2.8.133 GCC-EOC, page 2-116
EC1: 2.8.23 AS-MT, page 2-43	NE: 2.8.26 AUD-LOG-LOW, page 2-45	TRUNK: 2.8.134 GE-OOSYNC, page 2-116
EC1: 2.8.176 LOF (EC1), page 2-142	NE: 2.8.66 DATAFLT, page 2-73	TRUNK: 2.8.144 HI-LASERBIAS, page 2-121
EC1: 2.8.188 LOS (EC1, EC1-12), page 2-150	NE: 2.8.67 DBOSYNC, page 2-73	TRUNK: 2.8.146 HI-RXPOWER, page 2-123
EC1: 2.8.208 LPBKFACILITY (EC1), page 2-168	NE: 2.8.71 DUP-IPADDR, page 2-75	TRUNK: 2.8.148 HI-TXPOWER, page 2-125
EC1: 2.8.219 LPBKTERMINAL (EC1), page 2-173	NE: 2.8.72 DUP-NODENAME, page 2-76	TRUNK: 2.8.183 LO-RXPOWER, page 2-146
EC1: 2.8.294 RFI-L, page 2-213	NE: 2.8.85 ETH-LINKLOSS, page 2-86	TRUNK: 2.8.200 LO-TXPOWER, page 2-164
EC1: 2.8.305 SD-L, page 2-219	NE: 2.8.147 HITEMP, page 2-124	TRUNK: 2.8.172 LOCKOUT-REQ, page 2-139
EC1: 2.8.310 SF-L, page 2-223	NE: 2.8.150 I-HITEMP, page 2-126	TRUNK: 2.8.178 LOF (TRUNK), page 2-143

Table 2-8 Alarm Index by Logical Object (continued)

ENVALRM: 2.8.90 EXT, page 2-90	NE: 2.8.155 INTRUSION-PSWD, page 2-129	TRUNK: 2.8.180 LOM, page 2-144
EQPT: 2.8.22 AS-CMD, page 2-42	NE: 2.8.160 LAN-POL-REV, page 2-133	TRUNK: 2.8.195 LOS (TRUNK), page 2-156
EQPT: 2.8.23 AS-MT, page 2-43	NE: 2.8.260 OPTNTWMIS, page 2-192	TRUNK: 2.8.199 LOS-P (TRUNK), page 2-163
EQPT: 2.8.29 AUTORESET, page 2-46	NE: 2.8.318 SNTP-HOST, page 2-226	TRUNK: 2.8.216 LPBKFACILITY (TRUNK), page 2-171
EQPT: 2.8.43 BKUPMEMP, page 2-52	NE: 2.8.349 SYSBOOT, page 2-241	TRUNK: 2.8.227 LPBKTERMINAL (TRUNK), page 2-176
EQPT: 2.8.48 CARLOSS (EQPT), page 2-56	NE: 2.8.350 TEMP-MISM, page 2-241	TRUNK: 2.8.236 MANUAL-REQ-SPAN, page 2-179
EQPT: 2.8.56 CLDRESTART, page 2-64	OCH: 2.8.7 APC-CORRECTION-SKIPPED, page 2-33	TRUNK: 2.8.248 ODUK-1-AIS-PM, page 2-187
EQPT: 2.8.57 COMIOXC, page 2-64	OCH: 2.8.10 APC-OUT-OF-RANGE, page 2-34	TRUNK: 2.8.249 ODUK-2-AIS-PM, page 2-187
EQPT: 2.8.58 COMM-FAIL, page 2-65	OCH: 2.8.22 AS-CMD, page 2-42	TRUNK: 2.8.250 ODUK-3-AIS-PM, page 2-188
EQPT: 2.8.59 CONTBUS-A-18, page 2-66	OCH: 2.8.23 AS-MT, page 2-43	TRUNK: 2.8.251 ODUK-4-AIS-PM, page 2-188
EQPT: 2.8.60 CONTBUS-B-18, page 2-66	OCH: 2.8.196 LOS-O, page 2-157	2.8.252 ODUK-AIS-PM, page 2-188
EQPT: 2.8.61 CONTBUS-IO-A, page 2-67	OCH: 2.8.197 LOS-P (OCH), page 2-159	TRUNK: 2.8.253 ODUK-BDI-PM, page 2-189
EQPT: 2.8.62 CONTBUS-IO-B, page 2-68	OCH: 2.8.261 OPWR-HDEG, page 2-193	TRUNK: 2.8.254 ODUK-LCK-PM, page 2-189
EQPT: 2.8.63 CTNEQPT-MISMATCH, page 2-69	OCH: 2.8.262 OPWR-HFAIL, page 2-195	TRUNK: 2.8.255 ODUK-OCI-PM, page 2-190
EQPT: 2.8.64 CTNEQPT-PBPROT, page 2-70	OCH: 2.8.263 OPWR-LDEG, page 2-195	TRUNK: 2.8.256 ODUK-SD-PM, page 2-190
EQPT: 2.8.65 CTNEQPT-PBWORK, page 2-71	OCH: 2.8.264 OPWR-LFAIL, page 2-196	TRUNK: 2.8.257 ODUK-SF-PM, page 2-191
EQPT: 2.8.78 EQPT, page 2-82	OCH: 2.8.274 PARAM-MISM, page 2-201	TRUNK: 2.8.258 ODUK-TIM-PM, page 2-191
EQPT: 2.8.84 ERROR-CONFIG, page 2-85	OCH: 2.8.279 PORT-ADD-PWR-DEG-HI, page 2-205	TRUNK: 2.8.266 OTUK-AIS, page 2-197
EQPT: 2.8.87 EXCCOL, page 2-89	OCH: 2.8.280 PORT-ADD-PWR-DEG-LOW, page 2-205	TRUNK: 2.8.267 OTUK-BDI, page 2-197

Table 2-8 Alarm Index by Logical Object (continued)

EQPT: 2.8.92 FAILTOSW, page 2-91	OCH: 2.8.281 PORT-ADD-PWR-FAIL-HI, page 2-205	TRUNK: 2.8.268 OTUK-IAE, page 2-198
EQPT: 2.8.119 FORCED-REQ, page 2-110	OCH: 2.8.282 PORT-ADD-PWR-FAIL-LOW, page 2-205	TRUNK: 2.8.269 OTUK-LOF, page 2-199
EQPT: 2.8.147 HITEMP, page 2-124	OCH: 2.8.366 UNREACHABLE-TARGET-POWER, page 2-251	TRUNK: 2.8.270 OTUK-SD, page 2-199
EQPT: 2.8.151 IMPROPRMVL, page 2-127	OCH: 2.8.371 VOA-HDEG, page 2-253	TRUNK: 2.8.271 OTUK-SF, page 2-200
EQPT: 2.8.153 INHSWPR, page 2-128	OCH: 2.8.372 VOA-HFAIL, page 2-254	TRUNK: 2.8.272 OTUK-TIM, page 2-200
EQPT: 2.8.154 INHSWWKG, page 2-129	OCH: 2.8.373 VOA-LDEG, page 2-254	TRUNK: 2.8.273 OUT-OF-SYNC, page 2-201
EQPT: 2.8.157 IOSCFGCOPY, page 2-132	OCH: 2.8.374 VOA-LFAIL, page 2-255	TRUNK: 2.8.286 PTIM, page 2-208
EQPT: 2.8.172 LOCKOUT-REQ, page 2-139	OCHNC-CONN: 2.8.247 OCHNC-INC, page 2-187	TRUNK: 2.8.293 RFI, page 2-212
EQPT: 2.8.229 MAN-REQ, page 2-177	OCN: 2.8.2 AIS-L, page 2-31	TRUNK: 2.8.304 SD (TRUNK), page 2-219
EQPT: 2.8.230 MANRESET, page 2-177	OCN: 2.8.5 ALS, page 2-32	TRUNK: 2.8.309 SF (TRUNK), page 2-222
EQPT: 2.8.239 MEA (EQPT), page 2-181	OCN: 2.8.18 APS-INV-PRIM, page 2-40	TRUNK: 2.8.317 SIGLOSS, page 2-225
EQPT: 2.8.242 MEM-GONE, page 2-184	OCN: 2.8.19 APS-PRIM-FAC, page 2-40	TRUNK: 2.8.322 SQUELCHED, page 2-229
EQPT: 2.8.243 MEM-LOW, page 2-184	OCN: 2.8.21 APS-PRIM-SEC-MISM, page 2-41	TRUNK: 2.8.324 SSM-DUS, page 2-231
EQPT: 2.8.245 NO-CONFIG, page 2-186	OCN: 2.8.11 APSB, page 2-34	TRUNK: 2.8.325 SSM-FAIL, page 2-231
EQPT: 2.8.276 PEER-NORESPONSE, page 2-203	OCN: 2.8.12 APSCDFLTK, page 2-35	TRUNK: 2.8.326 SSM-LNC, page 2-232
EQPT: 2.8.285 PROTNA, page 2-208	OCN: 2.8.13 APSC-IMP, page 2-36	TRUNK: 2.8.327 SSM-OFF, page 2-232
EQPT: 2.8.287 PWR-FAIL-A, page 2-209	OCN: 2.8.14 APSCINCON, page 2-37	TRUNK: 2.8.328 SSM-PRC, page 2-232
EQPT: 2.8.288 PWR-FAIL-B, page 2-210	OCN: 2.8.15 APSCM, page 2-37	TRUNK: 2.8.329 SSM-PRS, page 2-233
EQPT: 2.8.289 PWR-FAIL-RET-A, page 2-210	OCN: 2.8.16 APSCNMIS, page 2-38	TRUNK: 2.8.330 SSM-RES, page 2-233
EQPT: 2.8.290 PWR-FAIL-RET-B, page 2-211	OCN: 2.8.17 APSIMP, page 2-39	TRUNK: 2.8.331 SSM-SDN-TN, page 2-233

Table 2-8 Alarm Index by Logical Object (continued)

EQPT: 2.8.302 RUNCFG-SAVENEED, page 2-217	OCN: 2.8.20 APSMM, page 2-40	TRUNK: 2.8.332 SSM-SETS, page 2-233
EQPT: 2.8.313 SFTWDOWN, page 2-224	OCN: 2.8.22 AS-CMD, page 2-42	TRUNK: 2.8.333 SSM-SMC, page 2-233
EQPT: 2.8.340 SWMTXMOD, page 2-235	OCN: 2.8.23 AS-MT, page 2-43	TRUNK: 2.8.334 SSM-ST2, page 2-234
EQPT: 2.8.376 WKSWPR, page 2-255	OCN: 2.8.28 AUTOLSROFF, page 2-45	TRUNK: 2.8.335 SSM-ST3, page 2-234
EQPT: 2.8.377 WTR, page 2-256	OCN: 2.8.44 BLSROSYNC, page 2-53	TRUNK: 2.8.336 SSM-ST3E, page 2-234
ESCON: 2.8.5 ALS, page 2-32	OCN: 2.8.86 E-W-MISMATCH, page 2-87	TRUNK: 2.8.337 SSM-ST4, page 2-234
ESCON: 2.8.22 AS-CMD, page 2-42	OCN: 2.8.76 EOC, page 2-79	TRUNK: 2.8.338 SSM-STU, page 2-235
ESCON: 2.8.23 AS-MT, page 2-43	OCN: 2.8.77 EOC-L, page 2-81	TRUNK: 2.8.339 SSM-TNC, page 2-235
ESCON: 2.8.92 FAILTOSW, page 2-91	OCN: 2.8.88 EXERCISE-RING-FAIL, page 2-89	TRUNK: 2.8.344 SYNC-FREQ, page 2-238
ESCON: 2.8.121 FORCED-REQ-SPAN, page 2-111	OCN: 2.8.89 EXERCISE-SPAN-FAIL, page 2-90	TRUNK: 2.8.345 SYNCLOSS, page 2-238
ESCON: 2.8.144 HI-LASERBIAS, page 2-121	OCN: 2.8.91 EXTRA-TRAF-PREEMPT, page 2-91	TRUNK: 2.8.351 TIM, page 2-242
ESCON: 2.8.146 HI-RXPOWER, page 2-123	OCN: 2.8.92 FAILTOSW, page 2-91	TRUNK: 2.8.352 TIM-MON, page 2-243
ESCON: 2.8.148 HI-TXPOWER, page 2-125	OCN: 2.8.94 FAILTOSWR, page 2-93	TRUNK: 2.8.363 UNC-WORD, page 2-248
ESCON: 2.8.183 LO-RXPOWER, page 2-146	OCN: 2.8.95 FAILTOSWS, page 2-95	TRUNK: 2.8.367 UT-COMM-FAIL, page 2-252
ESCON: 2.8.200 LO-TXPOWER, page 2-164	OCN: 2.8.107 FE-FRCDWKSWBK-SPAN, page 2-104	TRUNK: 2.8.368 UT-FAIL, page 2-252
ESCON: 2.8.172 LOCKOUT-REQ, page 2-139	OCN: 2.8.108 FE-FRCDWKSWPR-RING, page 2-104	TRUNK: 2.8.376 WKSWPR, page 2-255
ESCON: 2.8.189 LOS (ESCON), page 2-151	OCN: 2.8.109 FE-FRCDWKSWPR-SPAN, page 2-105	TRUNK: 2.8.377 WTR, page 2-256
ESCON: 2.8.209 LPBKFACILITY (ESCON), page 2-169	OCN: 2.8.111 FE-LOCKOUTOFPR-SPAN, page 2-106	TRUNK: 2.8.378 WVL-MISMATCH, page 2-256
ESCON: 2.8.220 LPBKTERMINAL (ESCON), page 2-173	OCN: 2.8.114 FE-MANWKSWBK-SPAN, page 2-107	VCG: 2.8.171 LOA, page 2-138

Table 2-8 Alarm Index by Logical Object (continued)

ESCON: 2.8.236 MANUAL-REQ-SPAN, page 2-179	OCN: 2.8.115 FE-MANWKSWPR-RING, page 2-108	VCG: 2.8.369 VCG-DEG, page 2-253
ESCON: 2.8.322 SQUELCHED, page 2-229	OCN: 2.8.116 FE-MANWKSWPR-SPAN, page 2-109	VCG: 2.8.370 VCG-DOWN, page 2-253
ESCON: 2.8.376 WKSWPR, page 2-255	OCN: 2.8.117 FEPRLF, page 2-109	VT-MON: 2.8.4 AIS-V, page 2-32
ESCON: 2.8.377 WTR, page 2-256	OCN: 2.8.120 FORCED-REQ-RING, page 2-110	VT-MON: 2.8.30 AUTOSW-AIS, page 2-47
EXT-SREF: 2.8.123 FRCDSWTOPRI, page 2-111	OCN: 2.8.121 FORCED-REQ-SPAN, page 2-111	VT-MON: 2.8.32 AUTOSW-LOP (VT-MON), page 2-48
EXT-SREF: 2.8.124 FRCDSWTOSEC, page 2-112	OCN: 2.8.128 FULLPASSTHR-BI, page 2-113	VT-MON: 2.8.37 AUTOSW-UNEQ (VT-MON), page 2-50
EXT-SREF: 2.8.125 FRCDSWTOTHIRD, page 2-112	OCN: 2.8.141 HELLO, page 2-120	VT-MON: 2.8.93 FAILTOSW-PATH, page 2-92
EXT-SREF: 2.8.232 MANSWTOPRI, page 2-178	OCN: 2.8.144 HI-LASERBIAS, page 2-121	VT-MON: 2.8.119 FORCED-REQ, page 2-110
EXT-SREF: 2.8.233 MANSWTOSEC, page 2-178	OCN: 2.8.145 HI-LASERTEMP, page 2-122	VT-MON: 2.8.172 LOCKOUT-REQ, page 2-139
EXT-SREF: 2.8.234 MANSWTOTHIRD, page 2-178	OCN: 2.8.146 HI-RXPOWER, page 2-123	VT-MON: 2.8.182 LOP-V, page 2-145
EXT-SREF: 2.8.341 SWTOPRI, page 2-237	OCN: 2.8.148 HI-TXPOWER, page 2-125	VT-MON: 2.8.229 MAN-REQ, page 2-177
EXT-SREF: 2.8.342 SWTOSEC, page 2-237	OCN: 2.8.158 KB-PASSTHR, page 2-132	VT-MON: 2.8.307 SD-V, page 2-220
EXT-SREF: 2.8.343 SWTOTHIRD, page 2-237	OCN: 2.8.159 KBYTE-APS-CHANNEL-FAIL URE, page 2-133	VT-MON: 2.8.312 SF-V, page 2-223
EXT-SREF: 2.8.346 SYNCPRI, page 2-239	OCN: 2.8.164 LASEREOL, page 2-135	VT-MON: 2.8.365 UNEQ-V, page 2-251
EXT-SREF: 2.8.347 SYNCSEC, page 2-240	OCN: 2.8.170 LKOUTPR-S, page 2-138	VT-MON: 2.8.376 WKSWPR, page 2-255
EXT-SREF: 2.8.348 SYNCTHIRD, page 2-240	OCN: 2.8.179 LO-LASERTEMP, page 2-144	VT-MON: 2.8.377 WTR, page 2-256
FAN: 2.8.80 EQPT-MISS, page 2-83	OCN: 2.8.183 LO-RXPOWER, page 2-146	VT-TERM: 2.8.4 AIS-V, page 2-32
FAN: 2.8.96 FAN, page 2-97	OCN: 2.8.200 LO-TXPOWER, page 2-164	VT-TERM: 2.8.24 AS-MT-OOG, page 2-43

Table 2-8 Alarm Index by Logical Object (continued)

FAN: 2.8.240 MEA (FAN), page 2-183	OCN: 2.8.172 LOCKOUT-REQ, page 2-139	VT-TERM: 2.8.166 LCAS-CRC, page 2-136
FAN: 2.8.244 MFGMEM, page 2-185	OCN: 2.8.177 LOF (OCN), page 2-143	VT-TERM: 2.8.167 LCAS-RX-FAIL, page 2-137
FC: 2.8.5 ALS, page 2-32	OCN: 2.8.193 LOS (OCN), page 2-153	VT-TERM: 2.8.168 LCAS-TX-ADD, page 2-137
FC: 2.8.22 AS-CMD, page 2-42	OCN: 2.8.215 LPBKFACILITY (OCN), page 2-171	VT-TERM: 2.8.169 LCAS-TX-DNU, page 2-138
FC: 2.8.23 AS-MT, page 2-43	OCN: 2.8.226 LPBKTERMINAL (OCN), page 2-175	VT-TERM: 2.8.180 LOM, page 2-144
FC: 2.8.49 CARLOSS (FC), page 2-58	OCN: 2.8.235 MANUAL-REQ-RING, page 2-178	VT-TERM: 2.8.182 LOP-V, page 2-145
FC: 2.8.92 FAILTOSW, page 2-91	OCN: 2.8.236 MANUAL-REQ-SPAN, page 2-179	VT-TERM: 2.8.259 OOU-TPT, page 2-192
FC: 2.8.97 FC-NO-CREDITS, page 2-98	OCN: 2.8.284 PRC-DUPID, page 2-207	VT-TERM: 2.8.278 PLM-V, page 2-205
FC: 2.8.121 FORCED-REQ-SPAN, page 2-111	OCN: 2.8.294 RFI-L, page 2-213	VT-TERM: 2.8.296 RFI-V, page 2-214
FC: 2.8.134 GE-OOSYNC, page 2-116	OCN: 2.8.297 RING-ID-MIS, page 2-215	VT-TERM: 2.8.306 SD-P, page 2-220
FC: 2.8.144 HI-LASERBIAS, page 2-121	OCN: 2.8.298 RING-MISMATCH, page 2-215	VT-TERM: 2.8.311 SF-P, page 2-223
FC: 2.8.146 HI-RXPOWER, page 2-123	OCN: 2.8.299 RING-SW-EAST, page 2-216	VT-TERM: 2.8.323 SQM, page 2-230
FC: 2.8.148 HI-TXPOWER, page 2-125	OCN: 2.8.300 RING-SW-WEST, page 2-216	VT-TERM: 2.8.354 TIM-V, page 2-244
FC: 2.8.183 LO-RXPOWER, page 2-146	OCN: 2.8.305 SD-L, page 2-219	VT-TERM: 2.8.365 UNEQ-V, page 2-251
FC: 2.8.200 LO-TXPOWER, page 2-164	—	—

2.5 DS3-12 E Line Alarms

Unlike the standard DS-3 card, which uses the unframed format exclusively, the DS3-12E card provides three choices: unframed, M13, or C Bit. The choice of framing format determines the line alarms that the DS3-12E card reports. The following table lists the line alarms reported under each format.

The choice of framing format does not affect the reporting of STS alarms. Regardless of format, the DS3-12E card reports the same STS alarms and conditions, listed in [Table 2-9](#), as the standard DS-3 card reports.

Table 2-9 DS3-12E Line Alarms

Alarm	UNFRAMED	M13	CBIT
LOS DS1 or DS3)	Yes	Yes	Yes
AIS	Yes	Yes	Yes
LOF (DS1 or DS3)	No	Yes	Yes
FE-IDLW	No	Yes	Yes
RAI	No	Yes	Yes
Terminal Lpbk (LPBKTERMINAL for DS1 or DS3)	Yes	Yes	Yes
Facility Lpbk (LPBKFACILITY for DS1 or DS3)	Yes	Yes	Yes
LPBKDS1FEAC or LPBKDS3FEAC	No	No	Yes
FE Common Equipment Failure-NSA (FE-DS1-NSA or FE-DS3-NSA)	No	No	Yes
FE Equipment Failure-SA (FE-DS3-SA)	No	No	Yes
FE-LOS	No	No	Yes
FE-LOF	No	No	Yes
FE-AIS	No	No	Yes
FE-IDLE	No	No	Yes
FE Equipment Failure-NSA (FE-EQPT-NSA)	No	No	Yes

2.6 Trouble Notifications

The ONS 15454 system reports trouble by utilizing standard alarm and condition characteristics, standard severities following the rules in Telcordia GR-253, and graphical user interface (GUI) state indicators. These notifications are described in the following paragraphs.

The ONS 15454 uses standard Telcordia categories to characterize levels of trouble. The system reports trouble notifications as alarms and status or descriptive notifications (if configured to do so) as conditions in the CTC Alarms window. Alarms typically signify a problem that the user needs to remedy, such as a loss of signal. Conditions do not necessarily require troubleshooting.

2.6.1 Alarm Characteristics

The ONS 15454 uses standard alarm entities to identify what is causing trouble. All alarms stem from hardware, software, environment, or operator-originated problems whether or not they affect service. Current alarms for the network, CTC session, node, or card are listed in the Alarms tab. (In addition, cleared alarms are also found in the History tab.)

2.6.2 Condition Characteristics

Conditions include any problem detected on an ONS 15454 shelf. They can include standing or transient notifications. A snapshot of all current raised, standing conditions on the network, node, or card can be retrieved in the CTC Conditions window or using TL1's set of RTRV-COND commands. (In addition, some but not all cleared conditions are also found in the History tab.)

For a comprehensive list of all conditions, refer to the *Cisco ONS SONET TL1 Command Guide*.

2.6.3 Severities

The ONS 15454 uses Telcordia-devised standard severities for alarms and conditions: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA) and Not Reported (NR). These are described below:

- A Critical alarm generally indicates severe, service-affecting trouble that needs immediate correction. Loss of traffic on an STS-1, which can hold 28 DS-1 circuits, would be a Critical (CR), Service-Affecting (SA) alarm.
- A Major (MJ) alarm is a serious alarm, but the trouble has less impact on the network. For example, loss of traffic on more than five DS-1 circuits is Critical, but loss of traffic on one to five DS-1 circuits is Major (MJ).
- Minor (MN) alarms generally are those that do not affect service. For example, the APS byte failure (APSB) alarm indicates that line terminating equipment detects a byte failure on the signal that could prevent traffic from properly executing a traffic switch.
- Not Alarmed (NA) conditions are information indicators, such as for free-run synchronization state (FRNGSYNC) or a forced-switch to primary (FRCSWTOPRI) timing event. They might or might not require troubleshooting, as indicated in the entries.
- Not Reported (NR) conditions occur as a secondary result of another event. For example, the alarm indication signal (AIS), with severity NR, is inserted by a downstream node when an LOS (CR or MJ) alarm occurs upstream. These conditions do not in themselves require troubleshooting, but are to be expected in the presence of primary alarms.

All alarm, condition, and unreported event severities listed in this manual are default profile settings. However in situations when traffic is not lost—such as when the alarm occurs on protected ports or circuits—alarms having Critical (CR) or Major (MJ) default severities can be demoted to lower severities such as Minor (MN) or Non-Service Affecting (NSA) as defined in Telcordia GR-474.

Severities can also be customized for an entire network or for single nodes, from the network level down to the port level by changing or downloading customized alarm profiles. These custom severities are subject to the standard severity-demoting rules given in Telcordia GR-474. Procedures for customizing alarm severities are located in the *Cisco ONS 15454 Procedure Guide* Chapter 7, “Manage Alarms.”

2.6.4 Service Effect

Service-Affecting (SA) alarms—those that interrupt service—might be Critical (CR), Major (MJ), or Minor (MN) severity alarms. In some cases the severity of an alarm might not correspond to its service effect. For example, the AUTOSW-LOP alarm for the VTMON object is minor but service-affecting because it indicates a traffic switch has occurred directing traffic away from a loss of circuit path. Non-Service Affecting (NSA) alarms always have a Minor (MN) default severity.

2.6.5 States

The Alarms or History tab state (ST) column indicate the disposition of the alarm or condition as follows:

- A raised (R) event is one that is active.
- A cleared (C) event is one that is no longer active.
- A transient (T) event is one that is automatically raised and cleared in CTC during system changes such as user login, logout, loss of connection to node view, etc. Transient events do not require user action.

**Note**

Transient events are not defined in this documentation release.

2.7 Safety Summary

This section covers safety considerations designed to ensure safe operation of the ONS 15454. Personnel should not perform any procedures in this chapter unless they understand all safety precautions, practices, and warnings for the system equipment. Some troubleshooting procedures require installation or removal of cards; in these instances users should pay close attention to the following caution.

**Caution**

Hazardous voltage or energy could be present on the backplane when the system is operating. Use caution when removing or installing cards.

Some troubleshooting procedures require installation or removal of OC-192 cards; in these instances users should pay close attention to the following warning.

**Warning**

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293

**Warning**

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056

**Warning**

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

**Warning**

Class 1 laser product. Statement 1008

**Warning**

Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard. Statement 206

**Warning**

The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment. Statement 207

2.8 Alarm Procedures

This section lists alarms alphabetically and includes some conditions commonly encountered when troubleshooting alarms. The severity, description, and troubleshooting procedure accompany each alarm and condition.

**Note**

When you check the status of alarms for cards, ensure that the alarm filter icon in the lower right corner is not indented. If it is, click it to turn it off. When you are done checking for alarms, you can click the alarm filter icon again to turn filtering back on. For more information about alarm filtering, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 7, “Manage Alarms.”

**Note**

When checking alarms, ensure that alarm suppression is not enabled on the card or port. For more information about alarm suppression, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 7, “Manage Alarms.”

2.8.1 AIS

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, DS3, FUDC, MSUDC, TRUNK

The Alarm Indication Signal (AIS) condition indicates that this node is detecting AIS in the incoming signal SONET overhead.

Generally, any AIS is a special SONET signal that communicates to the receiving node when the transmit node does not send a valid signal. AIS is not considered an error. It is raised by the receiving node on each input when it sees the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

**Note**

ONS 15454 DS-3 and EC-1 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided.

Clear the AIS Condition

-
- Step 1** Determine whether there are alarms on the upstream nodes and equipment, especially the “[LOS \(OCN\)](#)” alarm on page 2-153, or out-of-service (OOS,MT or OOS,DSBLD) ports.
- Step 2** Clear the upstream alarms using the applicable procedures in this chapter.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.2 AIS-L

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: EC1, EC1-12, OCN

The AIS Line condition indicates that this node is detecting line-level AIS in the incoming signal. This alarm is secondary to another alarm occurring simultaneously in an upstream node.

Generally, any AIS is a special SONET signal that communicates to the receiving node when the transmit node does not send a valid signal. AIS is not considered an error. It is raised by the receiving node on each input when it sees the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the AIS-L Condition

-
- Step 1** Complete the “[Clear the AIS Condition](#)” procedure on page 2-31.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.3 AIS-P

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

The AIS Path condition means that this node is detecting AIS in the incoming path. This alarm is secondary to another alarm occurring simultaneously in an upstream node.

Generally, any AIS is a special SONET signal that communicates to the receiving node when the transmit node does not send a valid signal. AIS is not considered an error. It is raised by the receiving node on each input when it sees the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the AIS-P Condition

-
- Step 1** Complete the “[Clear the AIS Condition](#)” procedure on page 2-31.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.4 AIS-V

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: VT-MON, VT-TERM

The AIS VT condition means that this node is detecting AIS in the incoming VT-level path.

Generally, any AIS is a special SONET signal that communicates to the receiving node when the transmit node does not send a valid signal. AIS is not considered an error. It is raised by the receiving node on each input when it sees the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

See the “[1.12.2 AIS-V on DS3XM-6 or DS3XM-12 Unused VT Circuits](#)” section on page 1-143 for more information.

Clear the AIS-V Condition

-
- Step 1** Complete the “[Clear the AIS Condition](#)” procedure on page 2-31.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.5 ALS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, AOTS, ESCON, FC, GE, ISC, OCN, TRUNK

The Automatic Laser Shutdown (ALS) condition occurs when a DWDM Optical Pre-amplifier (OPT-PRE) or Optical Booster (OPT-BST) Amplifier card is switched on. The turn-on process lasts approximately nine seconds, and the condition clears after approximately 10 seconds.



Note

ALS is an informational condition and does not require troubleshooting.

2.8.6 AMPLI-INIT

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Occurs only on DWDM (Software R4.5) nodes

The Amplifier Initialized condition occurs when an amplifier card (OPT-BST or OPT-PRE) is not able to calculate gain. This condition typically accompanies the “APC-DISABLED” alarm on page 2-33.

Clear the AMPLI-INIT Condition

-
- Step 1** Complete the “[Delete a Circuit](#)” procedure on page 2-272 on the most recently created circuit.
- Step 2** Recreate this circuit using the procedures in the *Cisco ONS 15454 Procedure Guide*.
- Step 3** If the condition does not clear, log onto <http://www.cisco.com/tac> for more information or call TAC (1 800 553-2447).
-

2.8.7 APC-CORRECTION-SKIPPED

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Automatic Power Control (APC) Correction Skipped condition occurs when the actual power level of a DWDM channel exceeds the threshold setting by 3 dBm or more. The APC compares actual power levels with power level thresholds every 10 minutes or after any channel allocation is performed. If the actual power level is above or below the setting within 3 dBm, APC corrects the level. If the actual power level exceeds the threshold by +3 dBm or –3 dBm, APC cannot correct the level and the APC-CORRECTION-SKIPPED condition is raised.

There is no operator action to resolve this condition. It stays raised until the power level problem is resolved and APC takes a normal reading. For more information about APC, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.



Note

APC-CORRECTION-SKIPPED is an informational condition and does not require troubleshooting.

2.8.8 APC-DISABLED

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The APC Disabled alarm occurs when the information related to the number of DWDM channels is not reliable. The alarm can occur when the any related alarms also occur: the “[AMPLI-INIT](#)” condition on page 2-32, the “[EQPT](#)” alarm on page 2-82, the “[IMPROPRMVL](#)” alarm on page 2-127, or the “[MEA \(EQPT\)](#)” alarm on page 2-181. If the alarm occurs with the creation of the first circuit, delete and recreate the circuit. For more information about APC, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the APC-DISABLED Condition

-
- Step 1** Complete the appropriate procedure to clear the main alarm:
- [Clear the EQPT Alarm, page 2-82](#)

- Clear the IMPROPRMVL Alarm, page 2-127
- Clear the MEA (EQPT) Alarm, page 2-181

- Step 2** If the alarm does not clear, complete the “Delete a Circuit” procedure on page 2-272 and then recreate it using procedures in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.9 APC-END

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The APC Terminated on Manual Request condition is raised when the APC application terminates after being manually launched from CTC or TL1. It is an informational condition. For more information about APC, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.



Note APC-END is an informational condition and does not require troubleshooting.

2.8.10 APC-OUT-OF-RANGE

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The APC Out of Range condition is raised on DWDM amplifier cards (OPT-PRE and OPT-BST); optical service channel cards (OSCM and OSC-CSM); multiplexer cards (32MUX-O); demultiplexer cards (32DMX, 32DMX-O), and optical add/drop multiplexer cards (AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, and AD-4B-xx.x) when the requested gain or attenuation setpoint cannot be set because it exceeds the port parameter range. For example, this condition is raised when APC attempts to set the OPT-BST gain higher than 20 dBm (the maximum set-point) or set the attenuation on the express variable optical attenuation (VOA) lower than 0dBm (the minimum set-point).

Clear the APC-OUT-OF-RANGE Condition

- Step 1** Provision the correct setpoint. For instructions, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. The condition clears when the APC setting is corrected and after APC does not detect any errors in its next cycle.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.11 APSB

- Default Severity: Minor (MN), Non-Service Affecting (NSA)

- Logical Object: OCN

The Automatic Protection Switching (APS) Channel Byte Failure alarm occurs when line terminating equipment detects protection switching byte failure or an invalid switching code in the incoming APS signal. Some older non-Cisco SONET nodes send invalid APS codes if they are configured in a 1+1 protection scheme with newer SONET nodes, such as the ONS 15454. These invalid codes cause an APSB on an ONS 15454.

-
- Step 1** Use an optical test set to examine the incoming SONET overhead to confirm inconsistent or invalid K bytes. For specific procedures to use the test set equipment, consult the manufacturer. If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment might not interoperate effectively with the ONS 15454.
- Step 2** If the alarm does not clear and the overhead shows inconsistent or invalid K bytes, you might need to replace the upstream cards for protection switching to operate properly. Complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#).

**Caution**

For the ONS 15454, removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

-
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.12 APSCDFLTk

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The APS Default K Byte Received alarm occurs during bidirectional line switched ring (BLSR) provisioning or when a BLSR is not properly configured, for example, when a four-node BLSR has one node configured as a path protection. When this misconfiguration occurs, a node in a path protection or 1+1 configuration does not send the two valid K1/K2 APS bytes anticipated by a system configured for BLSR. One of the bytes sent is considered invalid by the BLSR configuration. The K1/K2 byte is monitored by receiving equipment for link-recovery information.

Troubleshooting for APSCDFLTk is often similar to troubleshooting for the [“BLSROSYNC” alarm on page 2-53](#).

Clear the APSCDFLTk Alarm

-
- Step 1** Complete the [“Identify a BLSR Ring Name or Node ID Number” procedure on page 2-259](#) to verify that each node has a unique node ID number.

- Step 2** Repeat [Step 1](#) for all nodes in the ring.
- Step 3** If two nodes have the same node ID number, complete the [“Change a BLSR Node ID Number” procedure on page 2-259](#) to change one node ID number so that each node ID is unique.
- Step 4** If the alarm does not clear, verify correct configuration of east port and west port optical fibers. (See the [“E-W-MISMATCH” alarm on page 2-87](#).) West port fibers must connect to east port fibers and vice versa. The *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable,” provides a procedure for fiberizing BLSRs.
- Step 5** If the alarm does not clear and the network is a four-fiber BLSR, ensure that each protect fiber is connected to another protect fiber and each working fiber is connected to another working fiber. The software does not report any alarm if a working fiber is incorrectly attached to a protect fiber.
- Step 6** If the alarm does not clear, complete the [“Verify Node Visibility for Other Nodes” procedure on page 2-260](#).
- Step 7** If nodes are not visible, complete the [“Verify or Create Node Section DCC Terminations” procedure on page 2-272](#) to ensure that SONET data communications channel (SDCC) terminations exist on each node.
- Step 8** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.13 APSC-IMP

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

An Improper SONET APS Code alarm indicates three consecutive, identical frames containing:

- Unused code in bits 6 through 8 of byte K2.
- Codes that are irrelevant to the specific protection switching operation being requested.
- Requests that are irrelevant to the ring state of the ring (such as a span protection switch request in a two-fiber ring NE).
- ET code in K2 bits 6 through 8 received on the incoming span, but not sourced from the outgoing span.



Note

This alarm can occur on a VT tunnel when it does not have VT circuits provisioned. It can also occur when the exercise command or a lockout is applied to a span. An externally switched span does not raise this alarm because traffic is preempted.



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

Clear the APSC-IMP Alarm

- Step 1** Use an optical test set to determine the validity of the K byte signal by examining the received signal. For specific procedures to use the test set equipment, consult the manufacturer.



- Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

If the K byte is invalid, the problem is with upstream equipment and not in the reporting ONS 15454. Troubleshoot the upstream equipment using the procedures in this chapter, as applicable. If the upstream nodes are not ONS 15454s, consult the appropriate user documentation.

- Step 2** If the K byte is valid, verify that each node has a ring name that matches the other node ring names. Complete the “[Identify a BLSR Ring Name or Node ID Number](#)” procedure on page 2-259.
- Step 3** Repeat [Step 2](#) for all nodes in the ring.
- Step 4** If a node has a ring name that does not match the other nodes, make that node’s ring name identical to the other nodes. Complete the “[Change a BLSR Ring Name](#)” procedure on page 2-259.
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.14 APSCINCON

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

An APS Inconsistent alarm means that an inconsistent APS byte is present. The SONET overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15454, to switch the SONET signal from a working to a protect path. An inconsistent APS code occurs when three consecutive frames do not contain identical APS bytes. Inconsistent APS bytes give the receiving equipment conflicting commands about switching.

Clear the APSCINCON Alarm

- Step 1** Look for other alarms, especially the “[LOS \(OCN\)](#)” alarm on page 2-153, the “[LOF \(OCN\)](#)” alarm on page 2-143, or the “[AIS](#)” condition on page 2-30. Clearing these alarms clears the APSCINCON alarm.
- Step 2** If an APSINCON alarm occurs with no other alarms, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.15 APSCM

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

The APS Channel Mismatch alarm occurs when the ONS 15454 expects a working channel but receives a protect channel. In many cases, the working and protect channels are crossed and the protect channel is active. If the fibers are crossed and the working line is active, the alarm does not occur. The APSCM alarm occurs only on the ONS 15454 when bidirectional protection is used on OC-N cards in a 1+1 configuration.



Warning

On the ONS 15454 OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

Clear the APSCM Alarm

Step 1 Verify that the working-card channel fibers are physically connected directly to the adjoining node working-card channel fibers.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the fibers are correctly connected, verify that the protection-card channel fibers are physically connected directly to the adjoining node protection-card channel fibers.

Step 3 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.16 APSCNMIS

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

The APS Node ID Mismatch alarm occurs when the source node ID contained in the incoming APS channel K2 byte is not present in the ring map. The APSCNMIS alarm could occur and clear when a BLSR is being provisioned. If so, you can disregard the temporary occurrence. If the APSCNMIS remains, the alarm clears when a K byte with a valid source node ID is received.

Clear the APSCNMIS Alarm

-
- Step 1** Complete the “[Identify a BLSR Ring Name or Node ID Number](#)” procedure on page 2-259 to verify that each node has a unique node ID number.
- Step 2** If the Node ID column contains any two nodes with the same node ID listed, record the repeated node ID.
- Step 3** Click **Close** in the Ring Map dialog box.
- Step 4** If two nodes have the same node ID number, complete the “[Change a BLSR Node ID Number](#)” procedure on page 2-259 to change one node ID number so that each node ID is unique.



Note If the node names shown in the network view do not correlate with the node IDs, log into each node and click the **Provisioning > BLSR** tabs. The BLSR window shows the node ID of the login node.



Note Applying and removing a lockout on a span causes the ONS node to generate a new K byte. The APSCNMIS alarm clears when the node receives a K byte containing the correct node ID.

- Step 5** If the alarm does not clear, use the “[Initiate a Lock Out on a BLSR Protect Span](#)” procedure on page 2-266 to lockout the span.
- Step 6** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-267 to clear the lockout.
- Step 7** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.17 APSIMP

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The APS Invalid Mode condition occurs if a 1+1 protection group is not properly configured at both nodes to send or receive the correct APS byte. A node that is either configured for no protection or is configured for path protection or BLSR protection does not send the right K2 APS byte anticipated by a system configured for 1+1 protection. The 1+1 protect port monitors the incoming K2 APS byte and raises this alarm if it does not receive the byte.

The condition is superseded by an APS, APSCM, or APSMM. It is not superseded by AIS or remote defect indication (RDI) line alarms. It clears when the port receives a valid code for 10 ms.

Clear the APSIMP Condition

-
- Step 1** Check the configuration of the other node in the 1+1 protection group. If the remote node is not configured for 1+1 protection, create the group. For instructions, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 4, “Turn Up Node.”

- Step 2** If the other end of the group is properly configured or the alarm does not clear after you have provisioned the group correctly, verify that the working ports and protect ports are cabled correctly.
- Step 3** Ensure that both protect ports are configured for SONET.
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.18 APS-INV-PRIM

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Optimized 1+1 APS Primary Facility condition occurs on OC-N cards in an optimized 1+1 protection system if the incoming primary section header does not indicate whether it is primary or secondary.



Note

APS-INV-PRIM is an informational condition and does not require troubleshooting. If the APS switch is related to other alarms, troubleshoot these alarms as necessary using the procedures in this chapter.

2.8.19 APS-PRIM-FAC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Optimized 1+1 APS Invalid Primary Section condition occurs on OC-N cards in an optimized 1+1 protection system if there is an APS status switch between the primary and secondary facilities to identify which port is primary.



Note

APS-INV-PRIM is an informational condition and does not require troubleshooting. If the APS switch is related to other alarms, troubleshoot these alarms as necessary using the procedures in this chapter.

Clear the APS-PRIM-FAC Condition

- Step 1** This condition clears when the card receives a valid primary section indication (1 or 2).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.20 APSMM

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

An APS Mode Mismatch failure alarm occurs on OC-N cards when there is a mismatch of the protection switching schemes at the two ends of the span, such as being bidirectional and unidirectional at each end. Each end of a span must be provisioned the same way: bidirectional and bidirectional, or unidirectional and unidirectional. APSMM can also occur if a non-Cisco vendor's equipment is provisioned as 1:N and the ONS 15454 is provisioned as 1+1.

If one end is provisioned for 1+1 protection switching and the other is provisioned for path protection switching, an APSMM alarm occurs in the ONS 15454 that is provisioned for 1+1 protection switching.

Clear the APSMM Alarm

-
- Step 1** For the reporting ONS 15454, display node view and verify the protection scheme provisioning:
- Click the **Provisioning > Protection** tabs.
 - Click the 1+1 protection group configured for the OC-N cards.
The chosen protection group is the protection group optically connected (with data communications channel, or DCC, connectivity) to the remote node.
 - Click **Edit**.
 - Record whether the Bidirectional Switching check box is checked.
- Step 2** Click **OK** in the Edit Protection Group dialog box.
- Step 3** Log into the remote-node node and verify that the OC-N 1+1 protection group is provisioned.
- Step 4** Verify that the Bidirectional Switching check box matches the checked or unchecked condition of the box recorded in [Step 1](#). If not, change it to match.
- Step 5** Click **Apply**.
- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.21 APS-PRIM-SEC-MISM

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Optimized 1+1 APS Primary Section Mismatch condition occurs on OC-N cards in an optimized 1+1 protection system if there is a mismatch between the primary section of the local node facility and the primary section of the remote-node facility.

Clear the APS-PRIM-SEC-MISM Alarm

-
- Step 1** Ensure that the local node and remote-node ports are correctly provisioned with the same way. For more information about optimized 1+1 configurations, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 4, "Turn Up Node."

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.22 AS-CMD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, AOTS, BPLANE, CE100T, DS1, DS3, E100T, E1000F, EC1, EC1-12, EQPT, ESCON, FC, FCMR, G1000, GE, GFP-FAC, ISC, ML100T, ML1000, NE, OCH, OCN, OMS, OTS, PPM, PWR, TRUNK

The Alarms Suppressed by User Command condition applies to the network element (NE object), backplane, a single card, or a port on a card. It occurs when alarms are suppressed for that object and its subordinate objects. For example, suppressing alarms on a card also suppresses alarms on its ports.

Clear the AS-CMD Condition

- Step 1** For all nodes, in node view, click the **Conditions** tab.
- Step 2** Click **Retrieve**. If you have already retrieved conditions, look under the Object column and Eqpt Type column and note what entity the condition is reported against, such as a port, slot, or shelf.
- If the condition is reported against a slot and card, alarms were either suppressed for the entire card or for one of the ports. Note the slot number and continue with [Step 3](#).
 - If the condition is reported against the backplane, go to [Step 7](#).
 - If the condition is reported against the NE object, go to [Step 8](#).
- Step 3** Determine whether alarms are suppressed for a port and if so, raise the suppressed alarms:
- a. Double-click the card to display the card view.
 - b. Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.
 - If the Suppress Alarms column check box is checked for a port row, deselect it and click **Apply**.
 - If the Suppress Alarms column check box is not checked for a port row, click **View > Go to Previous View**.
- Step 4** If the AS-CMD condition is reported for a card and not an individual port, in node view click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.
- Step 5** Locate the row number for the reported card slot.
- Step 6** Click the **Suppress Alarms** column check box to deselect the option for the card row.
- Step 7** If the condition is reported for the backplane, the alarms are suppressed for cards such as the ONS 15454 AIP that are not in the optical or electrical slots. To clear the alarm:
- a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.
 - b. In the backplane row, uncheck the Suppress Alarms column check box.
 - c. Click **Apply**.
- Step 8** If the condition is reported for the shelf, cards and other equipment are affected. To clear the alarm:
- a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs if you have not already done so.

- b. Click the **Suppress Alarms** check box located at the bottom of the window to deselect the option.
- c. Click **Apply**.

Step 9 If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.23 AS-MT

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, AOTS, BPLANE, CE100T, DS1, DS3, E100T, E1000F, EC1, EC1-12, EQPT, ESCON, FC, FCMR, GE, GFP-FAC, G1000, ISC, ML100T, ML1000, NE, OCH, OCN, OMS, OTS, PPM, PWR, TRUNK

The Alarms Suppressed for Maintenance Command condition applies to OC-N and electrical cards and occurs when a port is placed in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state for loopback testing operations.

Clear the AS-MT Condition

Step 1 Complete the [“Clear an OC-N Card Facility or Terminal Loopback Circuit” procedure on page 2-273](#).

Step 2 If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.24 AS-MT-OOG

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSTRM, VT-TERM

The Alarms Suppressed on an Out-Of-Group VCAT Member condition is raised on an STS or VT member of a VCAT group whenever the member is in the IDLE (AS-MT-OOG) admin state. This condition can be raised when a member is initially added to a group. In IDLE (AS-MT-OOG) state, all other alarms for the STS or VT are suppressed.

Clear the AS-MT-OOG Condition

Step 1 The AS-MT-OOG condition clears when an STS or VT member transitions to a different state from IDLE (AS-MT-OOG) or when it is removed completely from the VCAT group. It does not require troubleshooting unless it does not clear.

Step 2 If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.25 AUD-LOG-LOSS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The Audit Trail Log Loss condition occurs when the log is 100 percent full and that the oldest entries are being replaced as new entries are generated. The log capacity is 640 entries. The log must be off-loaded using the following procedure to make room for more entries.

Clear the AUD-LOG-LOSS Condition

-
- Step 1** In node view, click the **Maintenance > Audit** tabs.
- Step 2** Click **Retrieve**.
- Step 3** Click **Archive**.
- Step 4** In the Archive Audit Trail dialog box, navigate to the directory (local or network) where you want to save the file.
- Step 5** Enter a name in the File Name field.
- You do not have to assign an extension to the file. It is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.
- Step 6** Click **Save**.
- The 640 entries are saved in this file. New entries continue with the next number in the sequence, rather than starting over.
- Step 7** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.26 AUD-LOG-LOW

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The Audit Trail Log Low condition occurs when the audit trail log is 80 percent full.



Note

AUD-LOG-LOW is an informational condition and does not require troubleshooting.

2.8.27 AU-LOF

The Administrative Unit Loss of Multiframe alarm is not supported in this platform release. It is reserved for future development.

2.8.28 AUTOLSROFF

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: OCN

The Auto Laser Shutdown alarm occurs when the OC-192 card temperature exceeds 194 degrees F (90 degrees C). The internal equipment automatically shuts down the OC-192 laser when the card temperature rises to prevent the card from self-destructing.



Warning

On the ONS 15454 OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



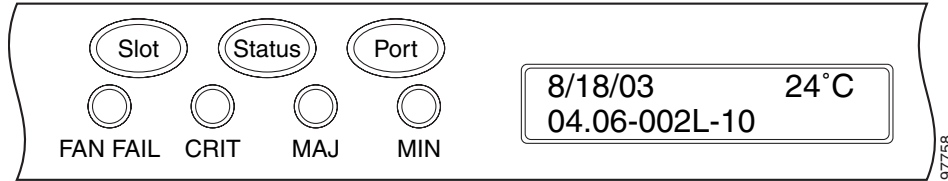
Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

Clear the AUTOLSROFF Alarm

-
- Step 1** View the temperature displayed on the ONS 15454 LCD front panel ([Figure 2-1](#)).

Figure 2-1 Shelf LCD Panel



Step 2 If the temperature of the shelf exceeds 194 degrees F (90 degrees C), the alarm should clear if you solve the ONS 15454 temperature problem. Complete the [“Clear the HITEMP Alarm” procedure on page 2-124](#).

Step 3 If the temperature of the shelf is under 194 degrees F (90 degrees C), the HITEMP alarm is not the cause of the AUTOLSROFF alarm. Complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the OC-192 card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 4 If card replacement does not clear the alarm, call Cisco TAC (1 800 553-2447) to discuss the case and if necessary open a returned materials authorization (RMA) on the original OC-192 card.

2.8.29 AUTORESET

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Automatic System Reset alarm occurs when you change an IP address or perform any other operation that causes an automatic card-level reboot.

AUTORESET typically clears after a card reboots (up to ten minutes). If the alarm does not clear, complete the following procedure.

Clear the AUTORESET Alarm

Step 1 Determine whether there are additional alarms that could have triggered an automatic reset. If there are, troubleshoot these alarms using the applicable section of this chapter.

Step 2 If the card automatically resets more than once a month with no apparent cause, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#).

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Caution**

For the ONS 15454, removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 3

If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.30 AUTOSW-AIS

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, VT-MON

The Automatic Path Protection Switch Caused by AIS condition indicates that automatic path protection switching occurred because of an AIS condition. The path protection is configured for revertive switching and reverts to the working path after the fault clears. The AIS also clears when the upstream trouble is cleared.

Generally, any AIS is a special SONET signal that communicates to the receiving node when the transmit node does not send a valid signal. AIS is not considered an error. It is raised by the receiving node on each input when it sees the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the AUTOSW-AIS Condition

Step 1

Complete the “[Clear the AIS Condition](#)” procedure on page 2-31.

Step 2

If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.31 AUTOSW-LOP (STSMON)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic Path Protection Switch Caused by LOP condition for the STS monitor (STSMON) indicates that automatic path protection switching occurred because of the “LOP-P” alarm on page 2-145. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-LOP (STSMON) Condition

- Step 1** Complete the “Clear the LOP-P Alarm” procedure on page 2-145.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.32 AUTOSW-LOP (VT-MON)

- Default Severity: Not Alarmed (NA), Service-Affecting (SA)
- Logical Object: VT-MON

The AUTOSW-LOP alarm for the virtual tributary monitor (VT-MON) indicates that automatic path protection switching occurred because of the “LOP-V” alarm on page 2-145. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-LOP (VT-MON) Condition

- Step 1** Complete the “Clear the LOP-V Alarm” procedure on page 2-146.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.33 AUTOSW-PDI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic Path Protection Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic path protection switching occurred because of a “PDI-P” alarm on page 2-201. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-PDI Condition

- Step 1** Complete the “Clear the PDI-P Condition” procedure on page 2-202.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.34 AUTOSW-SDBER

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic Path Protection Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that a signal degrade (SD) caused automatic path protection switching to occur. The path protection is configured for revertive switching and reverts to the working path when the SD is resolved.

Clear the AUTOSW-SDBER Condition

-
- Step 1** Complete the “[Clear the SD \(DS1, DS3\) Condition](#)” procedure on page 2-218.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.35 AUTOSW-SFBER

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic Path Protection Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a signal failure (SF) caused automatic path protection switching to occur. The path protection is configured for revertive switching and reverts to the working path when the SF is resolved.

Clear the AUTOSW-SFBER Condition

-
- Step 1** Complete the “[Clear the SF \(DS1, DS3\) Condition](#)” procedure on page 2-222.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.36 AUTOSW-UNEQ (STSMON)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Automatic Path Protection Switch Caused by Unequipped condition indicates that an UNEQ alarm caused automatic path protection switching to occur. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-UNEQ (STSMON) Condition

-
- Step 1** Complete the “[Clear the UNEQ-P Alarm](#)” procedure on page 2-249.

- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.37 AUTOSW-UNEQ (VT-MON)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: VT-MON

AUTOSW-UNEQ (VT-MON) indicates that the “UNEQ-V” alarm on page 2-251 alarm caused automatic path protection switching to occur. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-UNEQ (VT-MON) Condition

- Step 1** Complete the “Clear the UNEQ-V Alarm” procedure on page 2-251.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.38 AWG-DEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OTS

The Arrayed Waveguide Gratings (AWG) Degrade alarm occurs when a DWDM card heater-control circuit degrades. The heat variance can cause slight wavelength drift. The card does not need to be replaced immediately, but it should be at the next opportunity.

Clear the AWG-DEG Alarm

- Step 1** For the alarmed DWDM card, complete the “Physically Replace a Traffic Card” procedure on page 2-271 at the next opportunity.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.39 AWG-FAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: OTS

The AWG Failure alarm occurs when a DWDM card heater-control circuit completely fails. The circuit failure disables wavelength transmission. The card must be replaced to restore traffic.

Clear the AWG-FAIL Alarm

-
- Step 1** For the alarmed DWDM card, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.8.40 AWG-OVERTEMP

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: OTS

The AWG Over Temperature alarm is raised if a card having an AWG-FAIL alarm is not replaced and its heater-control circuit temperature exceeds 212 degrees F (100 degrees C). The card goes into protect mode and the heater is disabled.

Clear the AWG-OVERTEMP Alarm

-
- Step 1** Complete the “[Clear the AWG-FAIL Alarm](#)” procedure on page 2-51.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.8.41 AWG-WARM-UP

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OTS

The AWG Warm-Up condition occurs when a DWDM card heater-control circuit is attaining its operating temperature during startup. The condition lasts approximately 10 minutes but can vary somewhat from this period due to environmental temperature.



Note AWG-WARM-UP is an informational condition and does not require troubleshooting.

2.8.42 BAT-FAIL

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: PWR

The Battery Fail alarm occurs when one of the two power supplies (A or B) is not detected. This could be because the supply is removed or is not operational. The alarm does not distinguish between the individual power supplies, so on-site information about the conditions is necessary for troubleshooting.

Clear the BAT-FAIL Alarm

-
- Step 1** At the site, determine which battery is not present or operational.
- Step 2** Remove the power cable from the faulty supply. For instructions, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 1, “Install the Shelf and Backplane Cable,” and reverse the power cable installation procedure.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.43 BKUPMEMP

- Default Severity: Critical (CR), Service Affecting (SA)
- Logical Object: EQPT

The Primary Nonvolatile Backup Memory Failure alarm refers to a problem with the TCC2/TCC2P card flash memory. The alarm occurs when the TCC2/TCC2P is in use and has one of four problems:

- The flash manager fails to format a flash partition.
- The flash manager fails to write a file to a flash partition.
- There is a problem at the driver level.
- The code volume fails cyclic redundancy checking (CRC). CRC is a method to verify for errors in data transmitted to the TCC2/TCC2P.

The BKUPMEMP alarm can also cause the “EQPT” alarm on page 2-82. If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarm.



Caution

Software updating on a standby TCC2/TCC2P can take up to 30 minutes.

Clear the BKUPMEMP Alarm

-
- Step 1** Verify that both TCC2/TCC2P cards are powered and enabled by confirming lighted ACT/SBY LEDs on the TCC2/TCC2P cards.
- Step 2** Determine whether the active or standby TCC2/TCCP card has the alarm.
- Step 3** If both TCC2/TCCP cards are powered and enabled, reset the TCC2/TCCP card against which the alarm is raised. If the card is the active TCC2/TCCP card, complete the “[Reset an Active TCC2/TCC2P and Activate the Standby Card](#)” procedure on page 2-268. If the card is the standby TCC2/TCCP, use the substeps below.
- a. Right-click the standby TCC2/TCCP card in CTC.
 - b. Choose **Reset Card** from the shortcut menu.
 - c. Click **Yes** in the Are You Sure dialog box. The card resets, the FAIL LED blinks on the physical card.
 - d. Wait ten minutes to verify that the card you reset completely reboots.

- Step 4** If the TCC2/TCC2P card you reset does not reboot successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-270](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-271](#).

2.8.44 BLSROSYNC

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

The BLSR Out Of Synchronization alarm occurs during BLSR setup when you attempt to add or delete a circuit, and a working ring node loses its DCC connection because all transmit and receive fiber has been removed. CTC cannot generate the ring table and causes the BLSROSYNC alarm.



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057



Note

This alarm can also be expected when upgrading to Release 5.0 when the ring identifier is updated.

Clear the BLSROSYNC Alarm

- Step 1** Reestablish cabling continuity to the node reporting the alarm. Refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable,” for cabling information to reestablish the DCC.



Note

To verify cable continuity, follow site practices.

When the DCC is established between the node and the rest of the BLSR, it becomes visible to the BLSR and should be able to function on the circuits.

- Step 2** If alarms occur when you have provisioned the DCCs, see the [“2.8.76 EOC” section on page 2-79](#).
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.45 BPV

- Default Severity: Minor (MN), Service-Affecting (SA)
- Logical Object: BITS

The 64K Clock Bipolar Density Violation alarm is raised on the TCC2P card if there is a frequency variation in the 8K BITS clock. The TCC2P card contains an 8K clock and a 64K clock. Each has some bipolar variation, which is normal. This alarm is raised on the 8K clock if that variation discontinues. The BPV alarm is demoted by an LOF or LOS against the BITS clock.



Note

This alarm is not raised on the TCC2 card.

Clear the BPV Alarm

-
- Step 1** Reestablishing a normal BITS input signal clears the alarm. Clear any alarms on the incoming signal or against the BITS timing sources.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.46 CARLOSS (CE100T)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: CE100T

The Carrier Loss alarm is raised on CE-100T-8 cards in Mapper mode when there is a circuit failure due to link integrity. It does not get raised when a user simply puts the port In-Service. It has to be IS with circuit or loopback.

Clear the CARLOSS (CE100T) Alarm

-
- Step 1** Complete the [“Clear the CARLOSS \(G1000\) Alarm” procedure on page 2-59](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.47 CARLOSS (E100T, E1000F)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: E100T, E1000F

A Carrier Loss alarm on the LAN E-Series Ethernet card is the data equivalent of the [“LOS \(OCN\)” alarm on page 2-153](#). The Ethernet card has lost its link and is not receiving a valid signal. The most common causes of the CARLOSS alarm are a disconnected cable, an Ethernet Gigabit Interface

Converter (GBIC) fiber connected to an optical card rather than an Ethernet device, or an improperly installed Ethernet card. Ethernet card ports must be enabled for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

The CARLOSS alarm also occurs after a node database is restored. After restoration, the alarm clears in approximately 30 seconds after the node reestablishes Spanning Tree Protocol (STP).

Clear the CARLOSS (E100T, E1000F) Alarm

- Step 1** Verify that the fiber cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”



Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 2** If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card. For more information about fiber connections and terminations, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”

- Step 3** If no misconnection to an OC-N card exists, verify that the transmitting device is operational. If not, troubleshoot the device.

- Step 4** If the alarm does not clear, use an Ethernet test set to determine whether a valid signal is coming into the Ethernet port.

For specific procedures to use the test set equipment, consult the manufacturer.

- Step 5** If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port. To do this, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”

- Step 6** If a valid Ethernet signal is present, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-270](#) for the Ethernet card.

- Step 7** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the Ethernet card.



Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 8** If a CARLOSS alarm repeatedly appears and clears, use the following steps to examine the layout of your network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect.

An Ethernet manual cross-connect is used when another vendors' equipment sits between ONS 15454s, and the OSI/TARP-based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.

- Step 9** If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, then the reappearing alarm may be a result of mismatched STS circuit sizes in the set up of the manual cross-connect. If the Ethernet circuit is not part of a manual cross-connect, the following steps do not apply.
- a. Right-click anywhere in the row of the CARLOSS alarm.
 - b. Click **Select Affected Circuits** in the shortcut menu that appears.
 - c. Record the information in the type and size columns of the highlighted circuit.
 - d. From the examination of the layout of your network, determine which ONS 15454 and card host the Ethernet circuit at the other end of the Ethernet manual cross-connect by completing the following substeps:
 - Log into the ONS 15454 at the other end of the Ethernet manual cross-connect.
 - Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
 - Click the **Circuits** tab.
 - Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The Ethernet manual cross-connect circuit connects the Ethernet card to an OC-N card at the same node.
 - e. Use the information you recorded to determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size.

If one of the circuit sizes is incorrect, complete the “[Delete a Circuit](#)” procedure on page 2-272 and reconfigure the circuit with the correct circuit size. For more information, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 6, “Create Circuits and Tunnels.”
- Step 10** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.48 CARLOSS (EQPT)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: EQPT

A Carrier Loss on the LAN Equipment alarm generally occurs on OC-N cards when the ONS 15454 and the workstation hosting CTC do not have a TCP/IP connection. The problem involves the LAN or data circuit used by the RJ-45 (LAN) connector on the TCC2/TCC2P, or for the ONS 15454, the LAN backplane pin connection. The CARLOSS alarm does not involve an Ethernet circuit connected to an Ethernet port. The problem is in the connection and not CTC or the node.

On TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G or MXP_2.5G_10G cards, CARLOSS is also raised against trunk ports when ITU-T G.709 monitoring is turned off.

A TXP_MR_2.5G card can raise a CARLOSS alarm when the payload is incorrectly configured for the 10 Gigabit Ethernet or 1 Gigabit Ethernet payload data type.

**Warning**

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056

**Warning**

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

Clear the CARLOSS (EQPT) Alarm

- Step 1** If the reporting card is an MXP or TXP card in an ONS 15454 node, verify the data rate configured on the pluggable port module (PPM):
- Double-click the reporting MXP or TXP card.
 - Click the **Provisioning > Pluggable Port Modules** tabs.
 - View the Pluggable Port Modules area port listing in the **Actual Equipment** column and compare this with the contents of the Selected PPM area **Rate** column for the MXP or TXP multirate port.
 - If the rate does not match the actual equipment, you must delete and recreate the selected PPM. Select the PPM, click **Delete**, then click **Create** and choose the correct rate for the port rate.
- Step 2** If the reporting card is an OC-N card, verify connectivity by pinging the ONS 15454 that is reporting the alarm:
- If you are using a Microsoft Windows operating system, from the Start Menu choose **Programs > Accessories > Command Prompt**.
 - If you are using a Sun Solaris operating system, from the Common Desktop Environment (CDE) click the **Personal Application** tab and click **Terminal**.
 - For both the Sun and Microsoft operating systems, at the prompt type:


```
ping ONS-15454-IP-address
```

For example:

```
ping 198.168.10.10
```

If the workstation has connectivity to the ONS 15454, it shows a “reply from IP-Address” after the ping. If the workstation does not have connectivity, a “Request timed out” message appears.
- Step 3** If the ping is successful, an active TCP/IP connection exists. Restart CTC:
- Exit from CTC.
 - Reopen the browser.
 - Log into CTC.
- Step 4** Using optical test equipment, verify that proper receive levels are achieved. (For instructions to use optical test equipment, refer to the manufacturer documentation.)

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 5** Verify that the optical LAN cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”
- Step 6** If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card. For more information about fiber connections and terminations, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”
- Step 7** If you are unable to establish connectivity, replace the fiber cable with a new known-good cable. To do this, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”
- Step 8** If you are unable to establish connectivity, perform standard network or LAN diagnostics. For example, trace the IP route, verify cable continuity, and troubleshoot any routers between the node and CTC.



Note To verify cable continuity, follow site practices.

- Step 9** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.49 CARLOSS (FC)

The Carrier Loss alarm for Fibre Channel is not used in this platform in this release. It is reserved for future development.

2.8.50 CARLOSS (G1000)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: G1000

A Carrier Loss alarm on the LAN G-Series Ethernet card is the data equivalent of the “[LOS \(OCN\)](#)” alarm on [page 2-153](#). The Ethernet card has lost its link and is not receiving a valid signal.

CARLOSS on the G1000-4 card is caused by one of two situations:

- The G1000-4 port reporting the alarm is not receiving a valid signal from the attached Ethernet device. The CARLOSS can be caused by an improperly connected Ethernet cable or a problem with the signal between the Ethernet device and the G1000-4 port.
- If a problem exists in the end-to-end path (including possibly the remote-node G1000-4 card), it causes the reporting card to turn off the Gigabit Ethernet transmitter. Turning off the transmitter typically causes the attached device to turn off its link laser, which results in a CARLOSS on the reporting G1000-4 card. The root cause is the problem in the end-to-end path. When the root cause is cleared, the remote-node G1000-4 port turns the transmitter laser back on and clears the CARLOSS on the reporting card. If a turned-off transmitter causes the CARLOSS alarm, other alarms such as the “[TPTFAIL \(G1000\)](#)” alarm on [page 2-245](#) or OC-N alarms or conditions on the end-to-end path normally accompany the CARLOSS (G1000s) alarm.

Refer to the *<I_Ital>Cisco ONS 15454 Reference Manual* for a description of the G1000-4 card’s end-to-end Ethernet link integrity capability. Also see the “[TRMT](#)” alarm on [page 2-246](#) for more information about alarms that occur when a point-to-point circuit exists between two cards.

Ethernet card ports must be enabled for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

Clear the CARLOSS (G1000) Alarm

- Step 1** Verify that the fiber cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 2** If the fiber cable is correctly connected and attached, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.
- Step 3** If no misconnection to the OC-N card exists, verify that the attached transmitting Ethernet device is operational. If not, troubleshoot the device.
- Step 4** Verify that optical receive levels are within the normal range. The correct specifications are listed in the [“1.13.3 OC-N Card Transmit and Receive Levels”](#) section on page 1-154.
- Step 5** If the alarm does not clear, use an Ethernet test set to determine whether a valid signal is coming into the Ethernet port. For specific procedures to use the test set equipment, consult the manufacturer.
- Step 6** If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port. To do this, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”
- Step 7** If the alarm does not clear and link autonegotiation is enabled on the G1000-4 port, but the autonegotiation process fails, the card turns off its transmitter laser and reports a CARLOSS alarm. If link autonegotiation has been enabled for the port, determine whether there are conditions that could cause autonegotiation to fail:
- Confirm that the attached Ethernet device has autonegotiation enabled and is configured for compatibility with the asymmetric flow control on the card.
 - Confirm that the attached Ethernet device configuration allows reception of flow control frames.
- Step 8** If the alarm does not clear, disable and reenable the Ethernet port to attempt to remove the CARLOSS condition. (The autonegotiation process restarts.)
- Step 9** If the alarm does not clear and the [“TPTFAIL \(G1000\)”](#) alarm on page 2-245 is also reported, complete the [“Clear the TPTFAIL \(G1000\) Alarm”](#) procedure on page 2-245. If the TPTFAIL alarm is not reported, continue to the next step.



Note

When the CARLOSS and the TPTFAIL alarms are reported, the reason for the condition could be the G1000-4 card's end-to-end link integrity feature taking action on a remote failure indicated by the TPTFAIL alarm.

- Step 10** If the TPTFAIL alarm was not reported, determine whether a terminal (inward) loopback has been provisioned on the port:
- In node view, click the card to go to card view.
 - Click the **Maintenance > Loopback tabs**.

c. If the service state is listed as OOS-MA, LPBK&MT, a loopback is provisioned. Go to [Step 11](#).

Step 11 If a loopback was provisioned, complete the [“Clear Other DS-N Card, EC-1, or G1000 Card Loopbacks” procedure on page 2-274](#).

On the G1000-4, provisioning a terminal (inward) loopback causes the transmit laser to turn off. If an attached Ethernet device detects the loopback as a loss of carrier, the attached Ethernet device shuts off the transmit laser to the G1000-4 card. Terminating the transmit laser could raise the CARLOSS alarm because the loopbacked G1000-4 port detects the termination.

If the does not have a loopback condition, continue to [Step 12](#).

Step 12 If a CARLOSS alarm repeatedly appears and clears, the reappearing alarm could be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. Perform the following steps if the Ethernet circuit is part of a manual cross-connect:



Note An ONS 15454 Ethernet manual cross-connect is used when another vendors' equipment sits between ONS nodes, and the Open System Interconnection/Target Identifier Address Resolution Protocol (OSI/TARP)-based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.

- a. Right-click anywhere in the row of the CARLOSS alarm.
- b. Right-click or left-click **Select Affected Circuits** in the shortcut menu that appears.
- c. Record the information in the type and size columns of the highlighted circuit.
- d. Examine the layout of your network and determine which ONS 15454 and card host the Ethernet circuit at the other end of the Ethernet manual cross-connect by completing the following substeps:
 - Log into the node at the other end of the Ethernet manual cross-connect.
 - Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
 - Click the **Circuits** tab.
 - Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The cross-connect circuit connects the Ethernet card to an OC-N card at the same node.
- e. Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.
- f. If one of the circuit sizes is incorrect, complete the [“Delete a Circuit” procedure on page 2-272](#) and reconfigure the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* Chapter 6, “Create Circuits and Tunnels,” for detailed procedures to create circuits.

Step 13 If a valid Ethernet signal is present, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-270](#).

Step 14 If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the Ethernet card.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 15 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.51 CARLOSS (GE)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: GE

The Carrier Loss for Gigabit Ethernet (GE) alarm occurs on MXP and TXP card PPM clients supporting 1-Gbps or 10-Gbps traffic. The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

Clear the CARLOSS (GE) Alarm

- Step 1** Ensure that the GE client is correctly configured:
- a. Double-click the card to display the card view.
 - b. Click the **Provisioning > Pluggable Port Modules** tabs.
 - c. View the Pluggable Port Modules area port listing in the **Actual Equipment** column and compare this with the client equipment. If no PPM is provisioned, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable,” for provisioning instructions.
 - d. If a PPM has been created, view the contents of the Selected PPM area **Rate** column for the MXP or TXP MR card and compare this rate with the client equipment data rate. If the PPM rate is differently provisioned, select the PPM, click **Delete**, then click **Create** and choose the correct rate for the equipment type.
- Step 2** If there is no PPM misprovisioning, check for a fiber cut. An LOS alarm is also present. If there is an alarm, complete the “[Clear the LOS \(OCN\) Alarm](#)” procedure on page 2-153.
- Step 3** If there is no fiber cut or provisioning error, check the client-side equipment for any transmission errors on the line.
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.52 CARLOSS (ISC)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: ISC

The Carrier Loss for Inter-Service Channel (ISC) alarm occurs on TXP card PPM clients supporting ISC client traffic. The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

Clear the CARLOSS (ISC) Alarm

-
- Step 1** Complete the [“Clear the CARLOSS \(GE\) Alarm” procedure on page 2-61](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.53 CARLOSS (ML100T, ML1000)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: ML100T, ML1000

A Carrier Loss alarm on an ML-Series Ethernet card is the data equivalent of the [“LOS \(OCN\)” alarm on page 2-153](#). The Ethernet port has lost its link and is not receiving a valid signal.

A CARLOSS alarm occurs when the Ethernet port has been configured from the Cisco IOS command line interface (CLI) as a no-shutdown port and one of the following problems also occurs:

- The cable is not properly connected to the near or far port.
- Auto-negotiation is failing.
- The speed (10/100 ports only) is set incorrectly.

For information about provisioning ML-Series Ethernet cards from the Cisco IOS interface, refer to the *<I Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the CARLOSS (ML100T, ML1000) Alarm

-
- Step 1** Verify that the LAN cable is properly connected and attached to the correct port on the ML-Series card and on the peer Ethernet port. For more information about fiber connections and terminations, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”
- Step 2** If the alarm does not clear, verify that autonegotiation is set properly on the ML-Series card port and the peer Ethernet port.
- Step 3** If the alarm does not clear, verify that the speed is set properly on the ML-Series card port and the peer Ethernet port if you are using 10/100 ports.
- Step 4** If the alarm does not clear, the Ethernet signal is not valid, but the transmitting device is operational, replace the LAN cable connecting the transmitting device to the Ethernet port.
- Step 5** If the alarm does not clear, disable and reenble the Ethernet port by performing a “shutdown” and then a “no shutdown” on the Cisco IOS CLI. Autonegotiation restarts.
- Step 6** If the alarm does not clear, complete the [Create the Facility \(Line\) Loopback on the Source DS-1, DS-3, DS3N-12, DS3i-N-12, or EC1 Port, page 1-10](#) and test the loopback.
- Step 7** If the problem persists with the loopback installed, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-270](#).
- Step 8** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#).

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 9** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.54 CARLOSS (TRUNK)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

A Carrier Loss alarm on the optical trunk connecting to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_10E, TXPP_MR_2.5G, or MXP_2.5G_10G, MXP_2.5G_10E cards is raised when ITU-T G.709 monitoring is disabled.

Clear the CARLOSS (TRUNK) Alarm

- Step 1** Complete the “[Clear the LOS \(2R\) Alarm](#)” procedure on page 2-147.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.55 CASETEMP-DEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Case Temperature Degrade alarm is raised when a DWDM card temperature sensor detects an out-of-range external temperature at the shelf level. The working range for DWDM cards is from 23 degrees F (–5 degrees C) to 149 degrees F (65 degrees C).

Clear the CASETEMP-DEG Alarm

- Step 1** Check for and resolve the “[FAN](#)” alarm on page 2-97 if it is raised against the shelf.
- Step 2** If the alarm does not clear, complete the “[Inspect, Clean, and Replace the Reusable Air Filter](#)” procedure on page 2-275.

- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.56 CLDRESTART

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Cold Restart condition occurs when a card is physically removed and inserted, replaced, or when the ONS 15454 power is initialized.

Clear the CLDRESTART Condition

- Step 1** Complete the “[Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card](#)” procedure on [page 2-270](#).



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 2** If the condition fails to clear after the card reboots, complete the “[Remove and Reinsert \(Reseat\) Any Card](#)” procedure on [page 2-270](#).
- Step 3** If the condition does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on [page 2-271](#) for the card.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on [page 2-260](#) for commonly used traffic-switching procedures.



Note

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.57 COMIOXC

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The Input/Output Slot To Cross-Connect Communication Failure alarm is caused by the XC10G cross-connect card. It occurs when there is a communication failure for a traffic slot.

Clear the COMIOXC Alarm

-
- Step 1** Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-268 on the reporting XC10G cross-connect card. For the LED behavior, see the “[2.10.2 Typical Traffic Card LED Activity During Reset](#)” section on page 2-258.
- Step 2** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 3** If the CTC reset does not clear the alarm, move traffic off the reporting cross-connect card. Complete the “[Side Switch the Active and Standby XC10G Cross-Connect Cards](#)” procedure on page 2-269.
- Step 4** Complete the “[Remove and Reinsert \(Reseat\) Any Card](#)” procedure on page 2-270 for the reporting cross-connect card.
- Step 5** If the alarm does not clear, complete the “[Physically Replace an In-Service Cross-Connect Card](#)” procedure on page 2-271 for the reporting cross-connect card.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.58 COMM-FAIL

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Plug-In Module (card) Communication Failure indicates that there is a communication failure between the TCC2/TCC2P and the card. The failure could indicate a broken card interface.

Clear the COMM-FAIL Alarm

-
- Step 1** Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-268 for the reporting card.
- Step 2** If the alarm does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the card.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.3 CTC Card Resetting and Switching](#)” section on page 2-267 for commonly used traffic-switching procedures.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.59 CONTBUS-A-18

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

A Communication Failure from Controller Slot to Controller Slot alarm for the TCC2/TCC2P slot to TCC2/TCC2P slot occurs when the main processor on the TCC2/TCC2P in the first slot (TCC A) loses communication with the coprocessor on the same card. This applies to the Slot 7 TCC2/TCC2P.

Clear the CONTBUS-A-18 Alarm

- Step 1** Complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-270](#) to make the Slot 11 TCC2/TCC2P active.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 2** Wait approximately 10 minutes for the Slot 7 TCC2/TCC2P to reset as the standby TCC2/TCC2P. Verify that the ACT/SBY LED is correctly illuminated before proceeding to the next step. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 3** Position the cursor over the Slot 11 TCC2/TCC2P and complete the [“Reset an Active TCC2/TCC2P and Activate the Standby Card” procedure on page 2-268](#) to return the card to the active state.
- Step 4** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseat the card, complete the [“Reset an Active TCC2/TCC2P and Activate the Standby Card” procedure on page 2-268](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-271](#).
-

2.8.60 CONTBUS-B-18

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

A Communication Failure from Controller Slot to Controller Slot alarm for the TCC2/TCC2P slot to TCC2/TCC2P slot occurs when the main processor on the TCC2/TCC2P in the second slot (TCC B) loses communication with the coprocessor on the same card. This applies to the Slot 11 TCC2/TCC2P.

Clear the CONTBUS-B-18 Alarm

-
- Step 1** Complete the [“Reset an Active TCC2/TCC2P and Activate the Standby Card”](#) procedure on page 2-268 to make the Slot 7 TCC2/TCC2P active.
- Step 2** Wait approximately 10 minutes for the Slot 11 TCC2/TCC2P to reset as the standby TCC2/TCC2P. Verify that the ACT/SBY LED is correctly illuminated before proceeding to the next step. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 3** Position the cursor over the Slot 7 TCC2/TCC2P and complete the [“Reset an Active TCC2/TCC2P and Activate the Standby Card”](#) procedure on page 2-268 to return the Slot 11 TCC2/TCC2P card to the active state.
- Step 4** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseal the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card”](#) procedure on page 2-270. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card”](#) procedure on page 2-271.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

2.8.61 CONTBUS-IO-A

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

A TCCA to Shelf A Slot Communication Failure alarm occurs when the active Slot 7 TCC2/TCC2P (TCC A) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-A alarm can appear briefly when the ONS 15454 switches to the protect TCC2/TCC2P. In the case of a TCC2/TCC2P protection switch, the alarm clears after the other cards establish communication with the newly active TCC2/TCC2P. If the alarm persists, the problem is with the physical path of communication from the TCC2/TCC2P card to the reporting card. The physical path of communication includes the TCC2/TCC2P, the other card, and the backplane.

Clear the CONTBUS-IO-A Alarm

-
- Step 1** Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab and view the Eqpt Type column to reveal the provisioned type.
- If the actual card type and the provisioned card type do not match, see the [“MEA \(EQPT\)”](#) alarm on page 2-181 for the reporting card.
- Step 2** If the alarm object is any single card slot other than the standby Slot 11 TCC2/TCC2P, perform a CTC reset of the object card. Complete the [“Reset a Traffic Card in CTC”](#) procedure on page 2-268. For the LED behavior, see the [“2.10.2 Typical Traffic Card LED Activity During Reset”](#) section on page 2-258.
- Step 3** If the alarm object is the standby Slot 11 TCC2/TCC2P, complete the [“Reset a Traffic Card in CTC”](#) procedure on page 2-268 for it. The procedure is similar.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. (A reset standby card remains standby.)

If CONTBUS-IO-A is raised on several cards at the same time, complete the [“Reset an Active TCC2/TCC2P and Activate the Standby Card” procedure on page 2-268](#).

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

- Step 4** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 5** If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-270](#) for the reporting card.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 6** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-270](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-271](#).

2.8.62 CONTBUS-IO-B

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

A TCC B to Shelf Communication Failure alarm occurs when the active Slot 11 TCC2/TCC2P (TCC B) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-B alarm might appear briefly when the ONS 15454 switches to the protect TCC2/TCC2P. In the case of a TCC2/TCC2P protection switch, the alarm clears after the other cards establish communication with the newly active TCC2/TCC2P. If the alarm persists, the problem is with the physical path of communication from the TCC2/TCC2P card to the reporting card. The physical path of communication includes the TCC2/TCC2P, the other card, and the backplane.

Clear the CONTBUS-IO-B Alarm

- Step 1** Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab and view the Eqpt Type column to reveal the provisioned type.
- If the actual card type and the provisioned card type do not match, see the [“MEA \(EQPT\)” alarm on page 2-181](#) for the reporting card.
- Step 2** If the alarm object is any single card slot other than the standby Slot 7 TCC2/TCC2P, perform a CTC reset of the object card. Complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#). For the LED behavior, see the [“2.10.2 Typical Traffic Card LED Activity During Reset” section on page 2-258](#).
- Step 3** If the alarm object is the standby Slot 7 TCC2/TCC2P, complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for it. The procedure is similar.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. (A reset standby card remains standby.)

Step 4 If CONTBUS-IO-B is raised on several cards at the same time, complete the [“Reset an Active TCC2/TCC2P and Activate the Standby Card” procedure on page 2-268](#).

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 5 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 6 If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-270](#) for the reporting card.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 7 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-270](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-271](#).

2.8.63 CTNEQPT-MISMATCH

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Connection Equipment Mismatch (CTNEQPT-MISMATCH) condition is raised when there is a mismatch between the cross-connect card preprovisioned in the slot and the card actually present in the shelf. For example, one type of cross-connect card might be preprovisioned in Slot 10, but another might be physically installed. Or a card that is mismatched with the card. For example, CTNEQPT-MISMATCH is raised in when an XCVT card is replaced with an XC10G card.



Note

Cisco does not support configurations of unmatched cross-connect cards in Slot 8 and Slot 10, although this situation may briefly occur during the upgrade process.



Note

The cross-connect card you are replacing should not be the active card. (It can be in SBY state or otherwise not in use.)

If you upgrade a node to R5.0 and replace an XC with XCVT or XC10G, or an XCVT with an XC10G, the CTNEQPT-MISMATCH condition is raised but it is cleared when the upgrade process ends.



Note

During an upgrade, this condition occurs and is raised as its default severity, Not Alarmed (NA). However, after the upgrade has occurred, if you wish to change the condition's severity so that it is Not Reported (NR), you can do this by modifying the alarm profile used at the node. For more information about modifying alarm severities, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the CTNEQPT-MISMATCH Condition

-
- Step 1** Verify what kind of card is preprovisioned in the slot:
- a. In node view, click the **Inventory** tab.
 - b. View the slot's row contents in the Eqpt Type and Actual Eqpt Type columns.

The Eqpt Type column contains the equipment that is provisioned in the slot. The Actual Eqpt Type contains the equipment that is physically present in the slot. For example, Slot 8 might be provisioned for an XCVT card, which is shown in the Eqpt Type column, but an XC10G card could be physically present in the slot. The XC10G would be shown in the Actual Eqpt Type column.
- Step 2** Complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the mismatched card.
- Step 3** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.64 CTNEQPT-PBPROT

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The Interconnection Equipment Failure Protect Cross-Connect Card Payload Bus Alarm indicates a failure of the main payload between the protect ONS 15454 Slot 10 XC10G cross-connect card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card and the reporting traffic card, or the TCC2/TCC2P and the backplane.



Note

This alarm automatically raises and clears when the Slot 8 XC10G cross-connect card is reseated.



Caution

Software update on a standby TCC2/TCC2P can take up to 30 minutes.

Clear the CTNEQPT-PBPROT Alarm

-
- Step 1** If all traffic cards show CTNEQPT-PBPROT alarm:
- a. Complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-270](#) for the standby TCC2/TCC2P card.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- b. If the reseat fails to clear the alarm, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the standby TCC2/TCC2P.

**Caution**

Do not physically reseal an active TCC2/TCC2P. Doing so disrupts traffic.

- Step 2** If not all cards show the alarm, perform a CTC reset on the standby XC10G card. Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-268. For the LED behavior, see the “[2.10.2 Typical Traffic Card LED Activity During Reset](#)” section on page 2-258.
- Step 3** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- If the cross-connect reset is not complete and error-free or if the TCC2/TCC2P reboots automatically, call Cisco TAC (1 800 553-2447).
- Step 4** If the alarm does not clear, complete the “[Remove and Reinsert \(Reseat\) Any Card](#)” procedure on page 2-270 for the standby XC10G card.
- Step 5** Determine whether the card is an active card or standby card in a protection group. Click the node view **Maintenance > Protection** tabs, then click the protection group. The cards and their statuses are displayed in the list.
- Step 6** If the reporting traffic card is the active card in the protection group, complete the “[Initiate a 1:1 Card Switch Command](#)” procedure on page 2-263. After you move traffic off the active card, or if the reporting card is standby, continue with the following steps.
- Step 7** Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-268 on the reporting card. For the LED behavior, see the “[2.10.2 Typical Traffic Card LED Activity During Reset](#)” section on page 2-258.
- Step 8** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 9** If the alarm does not clear, complete the “[Remove and Reinsert \(Reseat\) Any Card](#)” procedure on page 2-270 for the reporting card.
- Step 10** Complete the “[Initiate a 1:1 Card Switch Command](#)” procedure on page 2-263 to switch traffic back.
- Step 11** If the alarm does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the reporting traffic card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” procedure on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 12** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.65 CTNEQPT-PBWORK

- Default Severity: Critical (CR), Service-Affecting (SA)

- Logical Object: EQPT

The Interconnection Equipment Failure Working Cross-Connect Card Payload Bus alarm indicates a failure in the main payload bus between the ONS 15454 Slot 8 XC10G cross-connect card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card and the reporting traffic card, or the TCC2/TCC2P and the backplane.

**Note**

This alarm automatically raises and clears when the ONS 15454 Slot 10 XC10G cross-connect card is reseated.

Clear the CTNEQPT-PBWORK Alarm

- Step 1** If all traffic cards show CTNEQPT-PBWORK alarm:
- Complete the [“Reset an Active TCC2/TCC2P and Activate the Standby Card” procedure on page 2-268](#) for the active TCC2/TCC2P and then complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-270](#).
 - If the reseat fails to clear the alarm, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the TCC2/TCC2P card.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Caution**

Do not physically reseat an active TCC2/TCC2P card; it disrupts traffic.

- Step 2** If not all traffic cards show the alarm, complete the [“Side Switch the Active and Standby XC10G Cross-Connect Cards” procedure on page 2-269](#) for the active XC10G cross-connect card.
- Step 3** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for the reporting card. For the LED behavior, see the [“2.10.2 Typical Traffic Card LED Activity During Reset” section on page 2-258](#).
- Step 4** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 5** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-270](#) for the standby cross-connect card.
- Step 6** If the alarm does not clear and the reporting traffic card is the active card in the protection group, complete the [“Initiate a 1:1 Card Switch Command” procedure on page 2-263](#). If the card is standby, or if you have moved traffic off the active card, proceed with the following steps.
- Step 7** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for the reporting card. For the LED behavior, see the [“2.10.2 Typical Traffic Card LED Activity During Reset” section on page 2-258](#).
- Step 8** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 9** If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-270](#) for the reporting card.
- Step 10** If you switched traffic, complete the [“Initiate a 1:1 Card Switch Command” procedure on page 2-263](#) to switch it back.

Step 11 If the alarm does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the XC10G card.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 12 If the alarm does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the reporting traffic card.

Step 13 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.66 DATAFLT

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: NE

The Software Data Integrity Fault alarm occurs when the TCC2/TCC2P exceeds its flash memory capacity.



Caution

When the system reboots, the last configuration entered is not saved.

Clear the DATAFLT Alarm

Step 1 Complete the “[Reset an Active TCC2/TCC2P and Activate the Standby Card](#)” procedure on page 2-268.

Step 2 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.67 DBOSYNC

- Default Severity: Major (MJ), Service Affecting (SA)
- Logical Object: NE

The standby Database Out Of Synchronization alarm occurs when the standby TCC2/TCC2P “To be Active” database does not synchronize with the active database on the active TCC2/TCC2P.



Caution

If you reset the active TCC2/TCC2P card while this alarm is raised, you lose current provisioning.

Clear the DBOSYNC Alarm

-
- Step 1** Save a backup copy of the active TCC2/TCC2P database. Refer to the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node,” for instructions.
- Step 2** Make a minor provisioning change to the active database to see if applying a provisioning change clears the alarm:
- a. In node view, click the **Provisioning > General > General** tabs.
 - b. In the Description field, make a small change such as adding a period to the existing entry.
The change causes a database write but does not affect the node state. The write could take up to a minute.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.68 DS3-MISM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The DS-3 Frame Format Mismatch condition indicates a frame format mismatch on a signal transiting the ONS 15454 DS3XM-6 or DS3XM-12 card. The condition occurs when the provisioned line type and incoming signal frame format type do not match. For example, if the line type for a DS3XM-6 card is set to C Bit and the incoming signal frame format is detected as M13, then the ONS 15454 reports a DS3-MISM condition.

Clear the DS3-MISM Condition

-
- Step 1** Display the CTC card view for the reporting DS3XM-6 or DS3XM-12 card.
- Step 2** Click the **Provisioning > Line** tabs.
- Step 3** For the row on the appropriate port, verify that the Line Type column is set to match the expected incoming signal (C Bit or M13).
- Step 4** If the Line Type field does not match the expected incoming signal, select the correct Line Type in the drop-down list.
- Step 5** Click **Apply**.
- Step 6** If the condition does not clear after the user verifies that the provisioned line type matches the expected incoming signal, use an optical test set to verify that the actual signal coming into the ONS 15454 matches the expected incoming signal.
For specific procedures to use the test set equipment, consult the manufacturer.
- Step 7** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.69 DSP-COMM-FAIL

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The Digital Signal Processor (DSP) Communication Failure alarm indicates that there is a communications failure between an MXP or TXP card microprocessor and the on-board DSP chip that controls the trunk (or DWDM) port. This alarm typically occurs after a DSP code upgrade.

The alarm is temporary and does not require user action. The MXP or TXP card microprocessor attempts to restore communication with the DSP chip until the alarm is cleared.

If the alarm is raised for an extended period, the MXP or TXP card raises the “[DSP-FAIL](#)” alarm on [page 2-75](#), and could affect traffic.

**Note**

DSP-COMM-FAIL is an informational alarm and does not require troubleshooting.

2.8.70 DSP-FAIL

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The DSP Failure alarm indicates that a “[DSP-COMM-FAIL](#)” alarm on [page 2-75](#) has persisted for an extended period on an MXP or TXP card. It indicates that the card is faulty.

Clear the DSP-FAIL Alarm

- Step 1** Complete the “[Physically Replace a Traffic Card](#)” procedure on [page 2-271](#) for the reporting MXP or TXP card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on [page 2-260](#) for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.71 DUP-IPADDR

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: NE

The Duplicate IP Address alarm indicates that the alarmed node IP address is already in use within the same DCC area. When this happens, TC no longer reliably connects to either node. Depending on how the packets are routed, CTC may connect to either node (having the same IP address). If CTC has connected to both nodes before they shared the same address, it has two distinct NodeModel instances (keyed by the node ID portion of the MAC address).

Clear the DUP-IPADDR Alarm

-
- Step 1** Isolate the alarmed node from the other node having the same address:
- a. Connect to the alarmed node using the Craft port on the ONS 15454 chassis.
 - b. Begin a CTC session.
 - c. On the login dialog window, uncheck the **Network Discovery** check box.
- Step 2** In node view, click the **Provisioning > Network > General** tabs.
- Step 3** In the IP Address field, change the IP address to a unique number.
- Step 4** Click **Apply**.
- Step 5** Restart any CTC sessions that are logged into either of the formerly duplicated node IDs. (For instructions to log in or log out, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 3, “Set Up PC and Log Into the GUI.”)
- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.72 DUP-NODENAME

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: NE

The Duplicate Node Name alarm indicates that the alarmed node alphanumeric name is already being used within the same DCC area.

Clear the DUP-NODENAME Alarm

-
- Step 1** In node view, click the **Provisioning > General > General** tabs.
- Step 2** In the Node Name field, enter a unique name for the node.
- Step 3** Click **Apply**.
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.73 EHIBATVG

- Default Severity: Major (MJ), Service-Affecting (SA)

- Logical Object: PWR

The Extreme High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the extreme high power threshold. This threshold, with a default value of –56.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds. (For information about changing this threshold, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 4, “Turn Up Node.”)

Clear the EHIBATVG Alarm

-
- Step 1** The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.74 ELWBATVG

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: PWR

The Extreme Low Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage falls below the extreme low power threshold. This threshold, with a default value of –40.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains over the threshold for 120 seconds. (For information about changing this threshold, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 4, “Turn Up Node.”)

Clear the ELWBATVG Alarm

-
- Step 1** The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.75 ENCAP-MISMATCH-P

- Default Severity: Critical (CR), Service-Affecting
- Logical Object: STS-TRM

The Encapsulation C2 Byte Mismatch Path alarm applies to ML-Series Ethernet cards. It occurs when the first three following conditions are met and one of the last two is false:

- The received C2 byte is not 0x00 (unequipped).
- The received C2 byte is not a PDI value.
- The received C2 does not match the expected C2.
- The expected C2 byte is not 0x01 (equipped unspecified).
- The received C2 byte is not 0x01 (equipped unspecified).

(This is in contrast to PLM-P, which must meet all five criteria.) For an ENCAP-MISMATCH-P to be raised, there is a mismatch between the received and expected C2 byte, with either the expected byte or received byte value being 0x01.

An example of a situation that would raise ENCAP-MISMATCH-P is if a circuit created between two ML-Series cards has generic framing procedure (GFP) framing provisioned on one end and high-level data link control (HDLC) framing with LEX encapsulation provisioned on the other. The GFP framing card transmits and expects a C2 byte of 0x1B, while the HDLC framing card transmits and expects a C2 byte of 0x01.

A mismatch between the transmit and receive cards on any of the following parameters can cause the alarm:

- Mode (HDLC, GFP-F)
- Encapsulation (LEX, HDLC, PPP)
- CRC size (16 or 32)
- Scrambling state (on or off)

This alarm is demoted by a PLM-P or PLM-V condition.

**Note**

By default, an ENCAP-MISMATCH-P alarm causes an ML-Series card data link to go down. This behavior can be modified using the command line interface (CLI) command **no pos trigger defect encap**.

**Note**

For more information about the ML-Series Ethernet cards, refer to the *<I>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the ENCAP-MISMATCH-P Alarm

-
- Step 1** Ensure that the correct framing mode is in use on the receive card:
- a. In node view, double-click the receive ML-Series card to display the card view.
 - b. Click the **Provisioning > Card** tabs.
 - c. In the Mode drop-down list, ensure that the same mode (GFP or HDLC) is selected. If it is not, choose it and click **Apply**.
- Step 2** Ensure that the correct framing mode is in use on the transmit card, and that it is identical to the receiving card:
- a. In node view, double-click the transmit ML-Series card to display the card view.
 - b. Click the **Provisioning > Card** tabs.
 - c. In the Mode drop-down list, ensure that the same mode (GFP or HDLC) is selected. If it is not, choose it and click **Apply**.
- Step 3** If the alarm does not clear, use the CLI to ensure that the remaining settings are correctly configured on the ML-Series card:
- Encapsulation
 - CRC size
 - Scrambling state

To open the interface, click the **IOS** tab and click **Open IOS Command Line Interface (CLI)**. Refer to the *<I_Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* entries on all three of these topics to obtain the full configuration command sequences.

- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.76 EOC

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: OCN, TRUNK

The SONET DCC Termination Failure alarm occurs when the ONS 15454 loses its data communications channel. Although this alarm is primarily SONET, it can apply to DWDM. For example, the OSCM card can raise this alarm on its OC-3 section overhead.

The SDCCs consist of three bytes, D1 through D3, in the SONET overhead. The bytes convey information about Operation, Administration, Maintenance, and Provisioning (OAM&P). The ONS 15454 uses the DCC on the SONET section layer to communicate network management information.



Warning

On the ONS 15454 OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057



Note

If a circuit shows a partial state when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the EOC Alarm

- Step 1** If the “[LOS \(DS1\)](#)” alarm on page 2-148 is also reported, complete the “[Clear the LOS \(DS1\) Alarm](#)” procedure on page 2-148.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 2** If the “SF-L” condition on page 2-223 is reported, complete the “Clear the SF-L Condition” procedure on page 2-223.
- Step 3** If the alarm does not clear on the reporting node, verify the physical connections between the cards and the fiber-optic cables are configured to carry SDCC traffic. If they are not, correct them. For more information about fiber connections and terminations, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”
- If the physical connections are correct and configured to carry DCC traffic, verify that both ends of the fiber span have in-service (IS-NR) ports. Verify that the ACT/SBY LED on each OC-N card is green.
- Step 4** When the LEDs on the OC-N cards are correctly illuminated, complete the “Verify or Create Node Section DCC Terminations” procedure on page 2-272 to verify that the DCC is provisioned for the ports at both ends of the fiber span.
- Step 5** Repeat Step 4 at the adjacent nodes.
- Step 6** If DCC is provisioned for the ends of the span, verify that the port is active and in service:
- Confirm that the OC-N card shows a green LED in CTC or on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 - To determine whether the port is in service, double-click the card in CTC to display the card view.
 - Click the **Provisioning > Line** tabs.
 - Verify that the Admin State column lists the port as **IS**.
 - If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and click **IS** in the drop-down list. Click **Apply**.
- Step 7** For all nodes, if the card is in service, use an optical test set to determine whether signal failures are present on fiber terminations.
- For specific procedures to use the test set equipment, consult the manufacturer.

**Caution**

Using an optical test set disrupts service on the OC-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the “2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260 for commonly used switching procedures.

- Step 8** If no signal failures exist on terminations, measure power levels to verify that the budget loss is within the parameters of the receiver. See the “1.13.3 OC-N Card Transmit and Receive Levels” section on page 1-154 for non-DWDM card levels and refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for DWDM card levels.
- Step 9** If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated. For more information refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”
- Step 10** If fiber connectors are properly fastened and terminated, complete the “Reset an Active TCC2/TCC2P and Activate the Standby Card” procedure on page 2-268.
- Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Resetting the active TCC2/TCC2P switches control to the standby TCC2/TCC2P. If the alarm clears when the ONS 15454 node switches to the standby TCC2/TCC2P, the user can assume that the previously active card is the cause of the alarm.

- Step 11** If the TCC2/TCC2P reset does not clear the alarm, delete the problematic SDCC termination:
- From card view, click **View > Go to Previous View** if you have not already done so.
 - Click the **Provisioning > Comm Channels > SDCC** tabs.
 - Highlight the problematic DCC termination.
 - Click **Delete**.
 - Click **Yes** in the Confirmation Dialog box.
- Step 12** Recreate the SDCC termination. Refer to the *Cisco ONS 15454 Procedure Guide* Chapter 5, “Turn Up Network,” for instructions.
- Step 13** Verify that both ends of the DCC have been recreated at the optical ports.
- Step 14** If the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseal the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-270](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-271](#).

2.8.77 EOC-L

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: OCN, TRUNK

The Line DCC Termination Failure alarm occurs when the ONS 15454 loses its line data communications channel. For example, the OSCM card can raise this alarm on its OC-3 line overhead.

The LDCCs are nine bytes, D4 through D12, in the SONET overhead. The bytes convey information about OAM&P. The ONS 15454 uses the LDCCs on the SONET line layer to communicate network management information.



Warning

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

**Note**

If a circuit shows a partial status when the EOC-L alarm is raised, it occurs when the logical circuit is in place. The circuit is able to carry traffic when the DCC termination issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the EOC-L Alarm

- Step 1** Complete the [“Clear the EOC Alarm” procedure on page 2-79](#).
- Step 2** If the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-270](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Traffic Card” procedure on page 2-271](#).

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

2.8.78 EQPT

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: AICI-AEP, AICI-AIE, EQPT, PPM

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card. If the EQPT alarm occurs with a BKUPMEMP alarm, refer to the [“2.8.43 BKUPMEMP” section on page 2-52](#). The BKUPMEMP procedure also clears the EQPT alarm.

This alarm is also invoked if a diagnostic circuit detects a card application-specific integrated circuit (ASIC) failure. In this case, if the card is part of a protection group, an APS switch occurs. If the card is the protect card, switching is inhibited and a PROTNA alarm is raised. The standby path generates a path-type alarm.

Clear the EQPT Alarm

- Step 1** If traffic is active on the alarmed port, you might need to switch traffic away from it. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.
- Step 2** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for the reporting card. For the LED behavior, see the [“2.10.2 Typical Traffic Card LED Activity During Reset” section on page 2-258](#).
- Step 3** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED status. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 4** If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-270](#) for the reporting card.
- Step 5** If the physical reseat of the card fails to clear the alarm, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the reporting card.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.79 EQPT-DIAG

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

An Equipment-Diagnostic Failure alarm indicates that a software or hardware failure has occurred on the reporting card. This alarm can be raised against a traffic card or a cross-connect card.

Clear the EQPT-DIAG Alarm

- Step 1** If traffic is active on the alarmed card, you might need to switch traffic away from it. Refer to the “[2.11.5 Generic Signal and Circuit Procedures](#)” section on page 2-272 for procedures.
- Step 2** Complete the “[Remove and Reinsert \(Reseat\) Any Card](#)” procedure on page 2-270 for the alarmed card

**Caution**

If the card carries live traffic, reseating it can affect this traffic.

- Step 3** If the alarm does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 if it is raised against a traffic card, or complete the “[Physically Replace an In-Service Cross-Connect Card](#)” procedure on page 2-271 if the alarm is raised against the cross-connect card.
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.80 EQPT-MISS

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: FAN

The Replaceable Equipment or Unit Missing alarm is reported against the fan-tray assembly unit. It indicates that the replaceable fan-tray assembly is missing or not fully inserted. It might also indicate that the ribbon cable connecting the AIP to the system board is bad.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Clear the EQPT-MISS Alarm

-
- Step 1** If the alarm is reported against the fan, verify that the fan-tray assembly is present.
- Step 2** If the fan-tray assembly is present, complete the [“Replace the Fan-Tray Assembly” procedure on page 2-277](#).
- Step 3** If no fan-tray assembly is present, obtain a fan-tray assembly and refer to the “Install the Fan-Tray Assembly,” procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”
- Step 4** If the alarm does not clear, replace the ribbon cable from the AIP to the system board with a known-good ribbon cable.
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.81 ERFI-P-CONN

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

The Three-Bit (Enhanced) Remote Failure Indication Path Connectivity condition is triggered on DS-1, DS-3, or VT circuits when the [“UNEQ-P” alarm on page 2-249](#) and the [“TIM-P” alarm on page 2-243](#) are raised on the transmission signal.

Clear the ERFI-P-CONN Condition

-
- Step 1** Complete the [“Clear the UNEQ-P Alarm” procedure on page 2-249](#). This should clear the ERFI condition.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.82 ERFI-P-PAYLD

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

The Three-Bit ERFI Path Payload condition is triggered on DS-1, DS-3, or VT circuits when the [“PLM-P” alarm on page 2-204](#) is raised on the transmission signal.

Clear the ERFI-P-PAYLD Condition

-
- Step 1** Complete the “[Clear the PLM-P Alarm](#)” procedure on page 2-204. This should clear the ERFI condition.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.83 ERFI-P-SRVR

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

The Three-Bit ERFI Path Server condition is triggered on DS-1, DS-3, or VT circuits when the “[AIS-P](#)” condition on page 2-31 or the “[LOP-P](#)” alarm on page 2-145 is raised on the transmission signal.

Clear the ERFI-P-SRVR Condition

-
- Step 1** Complete the “[Clear the LOP-P Alarm](#)” procedure on page 2-145. This should clear the ERFI condition.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.84 ERROR-CONFIG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Error in Startup Configuration alarm applies to the ML-Series Ethernet cards. These cards process startup configuration files line by line. If one or more lines cannot be executed, the error causes the ERROR-CONFIG alarm. ERROR-CONFIG is not caused by hardware failure.

The typical reasons for an errored startup file are:

- The user stored the configuration for one type of ML-Series card in the database and then installed another type in its slot.
- The configuration file contained a syntax error on one of the lines.

**Note**

For information about provisioning the ML-Series Ethernet cards from the Cisco IOS interface, refer to the *<I>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the ERROR-CONFIG Alarm

-
- Step 1** If you have a different type of ML-Series card specified in the startup configuration file than what you have installed, create the correct startup configuration.

Follow the card provisioning instructions in the *<I_Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

- Step 2** Upload the configuration file to the TCC2/TCC2P:
- In node view, right-click the ML-Series card graphic.
 - Choose **IOS Startup Config** from the shortcut menu.
 - Click **Local > TCC** and navigate to the file location in the Open dialog box.
- Step 3** Complete the “Reset a Traffic Card in CTC” procedure on page 2-268.
- Step 4** If the alarm does not clear or if your configuration file was correct according to the installed card, start a Cisco IOS CLI for the card:
- Right click the ML-Series card graphic in node view.
 - Choose **Open IOS Connection** from the shortcut menu.



Note Open IOS Connection is not available unless the ML-Series card is physically installed in the shelf.

Follow the card provisioning instructions in the *<I_Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* to correct the errored configuration file line.

- Step 5** Execute the CLI command:

```
copy run start
```

The command copies the new card configuration into the database and clears the alarm.

- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.85 ETH-LINKLOSS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The Rear Panel Ethernet Link Removed condition, if enabled in the network defaults, is raised under the following conditions:

- The node.network.general.AlarmMissingBackplaneLAN field in NE default is enabled.
- The node is configured as a gateway network element (GNE).
- The backplane LAN cable is removed.

Clear the ETH-LINKLOSS Condition

- Step 1** To clear this alarm, reconnect the backplane LAN cable. Refer to the *Cisco ONS 15454 Procedure Guide* Chapter 1, “Install the Shelf and Backplane Cable,” for instructions to install this cable.

- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.86 E-W-MISMATCH

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

A Procedural Error Mismatch East/West Direction alarm occurs during BLSR setup, or when nodes in a ring have slots misconnected. An east slot can be misconnected to another east slot, or a west slot can be misconnected to another west slot. In most cases, the user did not connect the fibers correctly or the ring provisioning plan was flawed. You can physically reconnect the cable to the correct slots to clear the E-W-MISMATCH alarm. Alternately, you can delete and recreate the span in CTC to change the west line and east line designations. The CTC method clears the alarm, but could change the traditional east-west node connection pattern of the ring.

**Note**

The E-W-MISMATCH alarm also appears during the initial set up of a ring with its east-west slots configured correctly. If the alarm appears during the initial setup, the alarm clears itself shortly after the ring setup is complete.

**Note**

The lower-numbered slot at a node is traditionally labeled as the west slot and the higher numbered slot is labeled as the east slot. For example, Slot 6 is west and Slot 12 is east.

**Note**

The physical switch procedure is the recommend method of clearing the E-W-MISMATCH alarm. The physical switch method reestablishes the logical pattern of connection in the ring. However, you can also use CTC to recreate the span and identify the misconnected slots as east and west. The CTC method is useful when the misconnected node is not geographically near the troubleshooter.

Clear the E-W-MISMATCH Alarm with a Physical Switch

- Step 1** Diagram the ring setup, including nodes and spans, on a piece of paper or white board.
- Step 2** In node view, click **View > Go to Network View**.
- Step 3** Label each of the nodes on the diagram with the same name that appears on the network map.
- Step 4** Right-click each span to reveal the node name/slot/port for each end of the span.
- Step 5** Label the span ends on the diagram with the same information. For example, with Node1/Slot12/Port1—Node2/Slot6/Port1 (2F BLSR OC48, ring name=0), label the end of the span that connects Node 1 and Node 2 at the Node 1 end as Slot 12/Port 1. Label the Node 2 end of that same span Slot 6/Port 1.
- Step 6** Repeat Steps 4 and 5 for each span on your diagram.
- Step 7** Label the highest slot at each node **east** and the lowest slot at each node **west**.

Step 8 Examine the diagram. You should see a clockwise pattern of west slots connecting to east slots for each span. Refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable,” for more information about cabling the system.

Step 9 If any span has an east-to-east or west-to-west connection, physically switching the fiber connectors from the card that does not fit the pattern to the card that continues the pattern should clear the alarm.



Warning

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

Step 10 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Clear the E-W-MISMATCH Alarm in CTC

Step 1 Log into the misconnected node. A misconnected node has both ring fibers connecting it to its neighbor nodes misconnected.

Step 2 Click the **Maintenance > BLSR** tabs.

Step 3 From the row of information for the fiber span, complete the “[Identify a BLSR Ring Name or Node ID Number](#)” procedure on page 2-259 to identify the node ID, ring name, and the slot and port in the East Line column and West Line column. Record the above information.

Step 4 Click **View > Go to Network View**.

Step 5 Delete and recreate the BLSR:

- a. Click the **Provisioning > BLSR** tabs.
- b. Click the row from [Step 3](#) to select it and click **Delete**.
- c. Click **Create**.
- d. Fill in the ring name and node ID from the information collected in [Step 3](#).
- e. Click **Finish**.

Step 6 Display node view and click the **Maintenance > BLSR** tabs.

Step 7 Change the West Line field to the slot you recorded for the East Line in [Step 3](#).

Step 8 Change the East Line field to the slot you recorded for the West Line in [Step 3](#).

Step 9 Click **OK**.

- Step 10** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.87 EXCCOL

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Excess Collisions on the LAN alarm indicates that too many collisions are occurring between data packets on the network management LAN, and communications between the ONS 15454 and CTC could be affected. The network management LAN is the data network connecting the workstation running the CTC software to the TCC2/TCC2P card. The problem causing the alarm is external to the ONS 15454.

Troubleshoot the network management LAN connected to the TCC2/TCC2P for excess collisions. You might need to contact the system administrator of the network management LAN to accomplish the following steps.

Clear the EXCCOL Alarm

- Step 1** Verify that the network device port connected to the TCC2/TCC2P card has a flow rate set to 10 Mb, half-duplex.
- Step 2** If the port has the correct flow rate and duplex setting, troubleshoot the network device connected to the TCC2/TCC2P card and the network management LAN.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.88 EXERCISE-RING-FAIL

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Exercise Ring command issues ring protection switching of the requested channel without completing the actual bridge and switch. The EXERCISE-RING-FAIL condition is raised if the command was issued and accepted but the exercise did not take place.



- Note** If the exercise command gets rejected due to the existence of a higher-priority condition in the ring, EXERCISE-RING-FAIL is not reported.
-

Clear the EXERCISE-RING-FAIL Condition

- Step 1** Look for and clear, if present, the “LOF (OCN)” alarm on page 2-143, the “LOS (OCN)” alarm on page 2-153, or BLSR alarms.

- Step 2** Reissue the Exercise Ring command:
- a. Click the **Maintenance > BLSR** tabs.
 - b. Click the row of the affected ring under the West Switch column.
 - c. Select **Exercise Ring** in the drop-down list.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.89 EXERCISE-SPAN-FAIL

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Exercise Span command issues span switching of the requested channel without completing the actual bridge and switch. The EXERCISE-SPAN-FAIL alarm is raised if the command was issued and accepted but the exercise did not take place.



Note

If the exercise command gets rejected due to the existence of a higher-priority condition in the span or ring, EXERCISE-SPAN-FAIL is not reported.

Clear the EXERCISE-SPAN-FAIL Condition

- Step 1** Look for and clear, if present, the “[LOF \(OCN\)](#)” alarm on page 2-143, the “[LOS \(OCN\)](#)” alarm on page 2-153, or a BLSR alarm.
- Step 2** Reissue the Exercise Span command:
- a. Click the **Maintenance > BLSR** tabs.
 - b. Determine whether the card you would like to exercise is the west card or the east card.
 - c. Click the row of the affected span under the East Switch or West Switch column.
 - d. Select **Exercise Span** in the drop-down list.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.90 EXT

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: ENVALRM

A Failure Detected External to the NE alarm occurs because an environmental alarm is present. For example, a door could be open or flooding might have occurred.

Clear the EXT Alarm

-
- Step 1** In node view double-click the AIC or AIC-I card to display the card view.
 - Step 2** Double-click the AIC or AIC-I card **Maintenance > External Alarms** tab.
 - Step 3** Follow your standard operating procedure to remedy environmental conditions that cause alarms. The alarm clears when the situation is remedied.
 - Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.91 EXTRA-TRAF-PREEMPT

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

An Extra Traffic Preempted alarm occurs on OC-N cards in two-fiber and four-fiber BLSRs when low-priority traffic directed to the protect system has been preempted by a working system protection switch.

Clear the EXTRA-TRAF-PREEMPT Alarm

-
- Step 1** Verify that the protection switch has occurred by checking the Conditions tab.
 - Step 2** If a ring switch has occurred, clear the ring switch on the working system by following the appropriate alarm in this chapter. For more information about protection switches, refer to the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 or the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”
 - Step 3** If the alarm occurred on a four-fiber BLSR and the span switch occurred on this OC-N, clear the span switch on the working system.
 - Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.92 FAILTOSW

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN, TRUNK

The Failure to Switch to Protection condition occurs when a working electrical card cannot switch to the protect card in a protection group because another working electrical card with a higher-priority alarm has switched to the protect card.

Clear the FAILTOSW Condition

Step 1 Look up and troubleshoot the higher-priority alarm. Clearing the higher-priority condition frees the card and clears the FAILTOSW.



Note A higher-priority alarm is an alarm raised on the working DS-N card using the 1:N card protection group. The working DS-N card is reporting an alarm but not reporting a FAILTOSW condition.

Step 2 If the condition does not clear, replace the working electrical card that is reporting the higher-priority alarm by following the [“Physically Replace a Traffic Card” procedure on page 2-271](#). This card is the working electrical card using the protect card and not reporting FAILTOSW.

Replacing the working electrical card that is reporting the higher-priority alarm allows traffic to revert to the working slot and the card reporting the FAILTOSW to switch to the protect card.



Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 3 If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.93 FAILTOSW-PATH

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, VT-MON

The Fail to Switch to Protection Path condition occurs when the working circuit does not switch to the protection circuit on a path protection. Common causes of the FAILTOSW-PATH alarm include a missing or defective protect port, a lockout set on one of the path protection nodes, or path level alarms that would cause a path protection switch to fail including the [“AIS-P” condition on page 2-31](#), the [“LOP-P” alarm on page 2-145](#), the [“SD-P” condition on page 2-220](#), the [“SF-P” condition on page 2-223](#), and the [“UNEQ-P” alarm on page 2-249](#).

The [“LOF \(OCN\)” alarm on page 2-143](#), the [“LOS \(OCN\)” alarm on page 2-153](#), the [“SD-L” condition on page 2-219](#), or the [“SF-L” condition on page 2-223](#) can also occur on the failed path.

Clear the FAILTOSW-PATH Condition in a Path Protection Configuration

- Step 1** Look up and clear the higher-priority alarm. Clearing this alarm frees the standby card and clears the FAILTOSW-PATH condition. If the “AIS-P” condition on page 2-31, the “LOP-P” alarm on page 2-145, the “UNEQ-P” alarm on page 2-249, the “SF-P” condition on page 2-223, the “SD-P” condition on page 2-220, the “LOF (OCN)” alarm on page 2-143, the “LOS (OCN)” alarm on page 2-153, the “SD-L” condition on page 2-219, or the “SF-L” condition on page 2-223 are also occurring on the reporting port, complete the applicable alarm clearing procedure.



Note A higher-priority alarm is an alarm raised on the working DS-N card using the 1:N card protection group. The working DS-N card is reporting an alarm but not reporting a FAILTOSW condition.

- Step 2** If the condition does not clear, replace the active OC-N card that is reporting the higher-priority alarm. Complete the “Physically Replace a Traffic Card” procedure on page 2-271. Replacing the active OC-N card that is reporting the higher-priority alarm allows traffic to revert to the active slot. Reverting frees the standby card, which can then take over traffic from the card reporting the lower-priority alarm and the FAILTOSW-PATH condition.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260 for commonly used traffic-switching procedures.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.94 FAILTOSWR

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Fail to Switch to Protection Ring condition occurs when a ring switch did not complete because of internal APS problems.

FAILTOSWR clears in any of the following situations:

- A physical card pull of the active TCC2/TCC2P card (done under Cisco TAC supervision).
- A node power cycle.

- A higher-priority event such as an external switch command.
- The next ring switch succeeds.
- The cause of the APS switch (such as the “SD (DS1, DS3)” condition on page 2-217 or the “SF (DS1, DS3)” condition on page 2-221) clears.

**Warning**

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293

**Warning**

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056

**Warning**

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

Clear the FAILTOSWR Condition in a BLSR Configuration

- Step 1** Perform the Exercise Ring command on the reporting card:
- Click the **Maintenance > BLSR** tabs.
 - Click the row of the affected ring under the West Switch column.
 - Select **Exercise Ring** in the drop-down list.
- Step 2** If the condition does not clear, from the view menu, choose **Go to Network View**.
- Step 3** Look for alarms on OC-N cards that make up the ring or span and troubleshoot these alarms.
- Step 4** If clearing other alarms does not clear the FAILTOSWR condition, log into the local node.
- Step 5** Click the **Maintenance > BLSR** tabs.
- Step 6** Record the OC-N cards listed under West Line and East Line. Ensure that these OC-N cards and ports and port are active and in service:
- Verify the LED status: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 - Double-click the card in CTC to display the card view.
 - Click the **Provisioning > Line** tabs.
 - Verify that the Admin State column lists the port as IS.
 - If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.
- Step 7** If the OC-N cards are active and in service, verify fiber continuity to the ports on the recorded cards.



Note To verify fiber continuity, follow site practices.

- Step 8** If fiber continuity to the ports is okay, use an optical test set to verify that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

**Caution**

Using an optical test set disrupts service on the OC-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used switching procedures.

- Step 9** If the signal is valid, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”
- Step 10** If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the OC-N card receiver specifications. The “[1.13.3 OC-N Card Transmit and Receive Levels](#)” section on page 1-154 lists these specifications.
- Step 11** Repeat Steps 7 through 10 for any other ports on the card.
- Step 12** If the optical power level for all OC-N cards is within specifications, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the protect standby OC-N card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 13** If the condition does not clear after you replace the BLSR cards on the node one by one, repeat Steps 4 through 12 for each of the nodes in the ring.
- Step 14** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.95 FAILTOSWS



- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Failure to Switch to Protection Span condition signals an APS span switch failure. For a four-fiber BLSR, a failed span switch initiates a ring switch. If the ring switch occurs, the FAILTOSWS condition does not appear. If the ring switch does not occur, the FAILTOSWS condition appears. FAILTOSWS clears when one of the following situations occurs:

- A physical card pull of the active TCC2/TCC2P done under Cisco TAC supervision.
- A node power cycle.
- A higher-priority event such as an external switch command occurs.
- The next span switch succeeds.

- The cause of the APS switch (such as the “SD (DS1, DS3)” condition on page 2-217 or the “SF (DS1, DS3)” condition on page 2-221) clears.

Clear the FAILTOSWS Condition

-
- Step 1** Perform the Exercise Span command on the reporting card:
- Click the **Maintenance > BLSR** tabs.
 - Determine whether the card you would like to exercise is the west card or the east card.
 - Click the row of the affected span under the East Switch or West Switch column.
 - Select **Exercise Span** in the drop-down list.
- Step 2** If the condition does not clear, from the view menu, choose **Go to Network View**.
- Step 3** Look for alarms on OC-N cards that make up the ring or span and troubleshoot these alarms.
- Step 4** If clearing other alarms does not clear the FAILTOSWS condition, log into the local node.
- Step 5** Click the **Maintenance > BLSR** tabs.
- Step 6** Record the OC-N cards listed under West Line and East Line. Ensure that these OC-N cards are active and in service:
- Verify the LED status: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 - To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
 - Click the **Provisioning > Line** tabs.
 - Verify that the Admin State column lists the port as IS.
 - If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.
- Step 7** If the OC-N cards are active and in service, verify fiber continuity to the ports on the recorded cards.
-  **Note** To verify fiber continuity, follow site practices.
-
- Step 8** If fiber continuity to the ports is okay, use an optical test set to verify that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.
-  **Caution** Using an optical test set disrupts service on the OC-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used switching procedures.
-
- Step 9** If the signal is valid, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”
- Step 10** If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the OC-N card receiver specifications. The “[1.13.3 OC-N Card Transmit and Receive Levels](#)” section on page 1-154 lists these specifications.
- Step 11** Repeat Steps 7 through 10 for any other ports on the card.

- Step 12** If the optical power level for all OC-N cards is within specifications, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the protect standby OC-N card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 13** If the condition does not clear after you replace the BLSR cards on the node one by one, follow Steps 4 through 12 for each of the nodes in the ring.
- Step 14** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.96 FAN

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: FAN

The Fan Failure alarm indicates a problem with the fan-tray assembly. When the fan-tray assembly is not fully functional, the temperature of the ONS 15454 can rise above its normal operating range.

The fan-tray assembly contains six fans and needs a minimum of five working fans to properly cool the shelf. However, even with five working fans, the fan-tray assembly could need replacement because a sixth working fan is required for extra protection against overheating.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Clear the FAN Alarm

- Step 1** Determine whether the air filter needs replacement. Complete the “[Inspect, Clean, and Replace the Reusable Air Filter](#)” procedure on page 2-275.
- Step 2** If the filter is clean, complete the “[Replace the Alarm Interface Panel](#)” procedure on page 2-279.

**Note**

The fan should run immediately when correctly inserted.

- Step 3** If the fan does not run or the alarm persists, complete the “[Replace the Fan-Tray Assembly](#)” procedure on page 2-277.

- Step 4** If the replacement fan-tray assembly does not operate correctly, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).
-

2.8.97 FC-NO-CREDITS

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: FC, FCMR

The Fibre Channel Distance Extension Credit Starvation alarm occurs on storage access networking (SAN) Fibre Channel/Fiber Connectivity (FICON) FC_MR-4 cards when the congestion prevents the GFP transmitter from sending frames to the FC_MR-4 card port. For example, the alarm can be raised when an operator configures a card to autodetect framing credits but the card is not connected to an interoperable FC-SW-standards-based Fibre Channel/FICON port.

FC-NO-CREDITS is raised only if transmission is completely prevented. (If traffic is slowed but still passing, this alarm is not raised.) The alarm is raised in conjunction with the GFP-NO-BUFFERS alarm. For example, if the FC-NO-CREDITS alarm is generated at an FC_MR-4 data port, a GFP-NO-BUFFERS alarm might be raised at the upstream remote FC_MR-4 data port.

Clear the FC-NO-CREDITS Alarm

- Step 1** If the port is connected to a Fibre Channel/FICON switch, make sure it is configured for interoperation mode. Follow manufacturer instructions.
- Step 2** If the port is not connected to a switch, turn off Autodetect Credits:
- Double-click the FC_MR-4 card.
 - Click **Provisioning > Port > General**.
 - Under Admin State, click the cell and choose **OOS,MT**.
 - Click **Apply**.
 - Click the **Provisioning > Port > Distance Extension** tabs.
 - Uncheck the **Autodetect Credits** column check box.
 - Click **Apply**.
 - Click **Provisioning > Port > General**.
 - Under Admin State, click the cell and choose **IS**.
 - Click **Apply**.
- Step 3** Program the Credits Available value based on the buffers available on the connected equipment:



Note The NumCredits must be provisioned to a value smaller than or equal to the receive buffers or credits available on the connected equipment.

- Double-click the FC_MR-4 card.
- Click the **Provisioning > Port > Distance Extension** tabs.

- c. Enter a new value in the Credits Available column.
- d. Click **Apply**.

Step 4 If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.8.98 FE-AIS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far-End AIS condition occurs when an AIS has occurred at the remote node. FE-AIS usually occurs in conjunction with a downstream LOS alarm (see the “[LOS \(OCN\)](#)” alarm on page 2-153).

Generally, any AIS is a special SONET signal that communicates to the receiving node when the transmit node does not send a valid signal. AIS is not considered an error. It is raised by the receiving node on each input when it sees the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the FE-AIS Condition

Step 1 Complete the “[Clear the AIS Condition](#)” procedure on page 2-31.

Step 2 If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.99 FEC-MISM

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The Forward Error Correction (FEC) Mismatch alarm occurs if one end of a span using MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G cards is configured to use FEC and the other is not. FEC-MISM is related to ITU-T G.709 and is only raised against a trunk port.

Clear the FEC-MISM Alarm

Step 1 Double-click the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E or TXPP_MR_2.5G card.

Step 2 Click the **Provisioning > OTN > OTN Lines** tab.

Step 3 In the FEC column, click **Standard** or **Enhanced** if you desire to enable the monitoring, or **Disable** if you do not.

- Step 4** Verify that the remote-node card is configured the same way by repeating [Step 1](#) through [Step 3](#).
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.100 FE-DS1-MULTLOS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far-End Multiple DS-1 LOS Detected condition occurs when multiple DS-1 signals are lost on a remote-node DS-1 card.

The prefix FE means the main alarm is occurring at the remote-node node and not at the node reporting the FE-DS1-MULTLOS condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-MULTLOS Condition

- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an ONS 15454 FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.101 FE-DS1-NSA

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End DS-1 Equipment Failure Non-Service Affecting condition occurs when a remote-node DS-1 equipment failure occurs, but does not affect service because the port is protected and traffic is able to switch to the protect port.

The prefix FE means the main alarm is occurring at the remote-node node and not at the node reporting the FE-DS1-NSA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-NSA Condition

-
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an alarm from a card in an ONS 15454 Slot 12 of Node 1 could link to an alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.102 FE-DS1-SA

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End DS-1 Equipment Failure Service Affecting condition occurs when there is a remote-node equipment failure on a DS-1 card that affects service because traffic is unable to switch to the protect port.

The prefix FE means the main alarm is occurring at the remote-node node and not at the node reporting the FE-DS1-SA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-SA Condition

-
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an alarm from a card in Slot 12 of Node 1 could link to an alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.103 FE-DS1-SNGLLOS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far-End Single DS-1 LOS condition occurs when a single DS-1 signal is lost on remote-node DS-1 equipment (within a DS3). Signal loss also causes the “LOS (OCN)” alarm on page 2-153.

The prefix FE in an alarm or condition means the main alarm is occurring at the remote-node node and not at the node reporting the FE-DS1-SNGLLOS alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-SNGLLOS Condition

-
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could link to an alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.104 FE-DS3-NSA

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End DS-3 Equipment Failure Non-Service Affecting condition occurs when a remote-node ONS 15454 DS-3 equipment failure occurs in C-bit framing mode, but does not affect service because the port is protected and traffic is able to switch to the protect port.

The prefix FE means the main alarm is occurring at the remote-node node and not at the node reporting FE-DS3-NSA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS3-NSA Condition

-
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an alarm from a card in Slot 12 of Node 1 could link to an alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.105 FE-DS3-SA

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: DS3

The Far End DS-3 Equipment Failure Service Affecting condition occurs when there is a remote-node equipment failure on an ONS 15454 DS-3 card in C-bit framing mode that affects service because traffic is unable to switch to the protect port.

The prefix FE in an alarm or condition means the main alarm is occurring at the remote-node node and not at the node reporting the FE condition. Troubleshoot the FE alarm by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS3-SA Condition

-
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an alarm from a card in Slot 12 of Node 1 could link to an alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.106 FE-EQPT-NSA

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End Common Equipment Failure condition occurs when a non-service-affecting equipment failure is detected on remote-node DS-3 equipment.

The prefix FE occurs when the main alarm is occurring at the remote-node node and not at the node reporting the FE-EQPT-NSA alarm. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-EQPT-NSA Condition

-
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.107 FE-FRCDWKSWBK-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Forced Switch Back to Working—Span condition is raised on a remote-node 1+1 working port when it is Force switched to the working port.



Note

WKSWBK-type conditions apply only to revertive circuits.

The prefix FE means the main alarm is occurring at the remote-node node and not at the node reporting the FE-FRCDWKSWBK-SPAN condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the primary alarm clears.

Clear the FE-FRCDWKSWBK-SPAN Condition

-
- Step 1** Complete the “[Clear a 1+1 Protection Port Force or Manual Switch Command](#)” procedure on page 2-261 for the remote-node port.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.108 FE-FRCDWKSWPR-RING

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Ring Working Facility Forced to Switch to Protection condition occurs from a remote-node node when a BLSR is forced from working to protect using the Force Ring command.

The prefix FE means the main alarm is occurring at the remote-node node and not at the node reporting the FE-FRCDWKSWPR-RING condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the primary alarm clears.

Clear the FE-FRCDWKSWPR-RING Condition

-
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm.
- Step 4** If the FE-FRCDWKSWPR-RING condition does not also clear, complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-267.

- Step 5** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.109 FE-FRCDWKSWPR-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Working Facility Forced to Switch to Protection Span condition occurs from a remote-node node when a span on a four-fiber BLSR is forced from working to protect using the Force Span command.

The prefix FE means the main alarm is occurring at the remote-node node and not at the node reporting the FE-FRCDWKSWPR-SPAN condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-FRCDWKSWPR-SPAN Condition

-
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm.
- Step 4** If the FE-FRCDWKSWPR-SPAN condition does not also clear, complete the [“Clear a BLSR External Switching Command” procedure on page 2-267](#) for instructions.
- Step 5** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.110 FE-IDLE

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End Idle condition occurs when a remote-node node detects an idle DS-3 signal in C-bit framing mode.

The prefix FE in an alarm or condition occurs when the main alarm is occurring at the remote-node node and not at the node reporting the FE-IDLE condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. Both alarms clear when the main alarm clears.

Clear the FE-IDLE Condition

-
- Step 1** To troubleshoot the FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm by clearing the protection switch. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.111 FE-LOCKOUTOFPR-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far-End Lock Out of Protection Span condition occurs when a BSLR span is locked out of the protection system from a remote-node node using the Lockout Protect Span command.

The prefix FE means the main alarm is occurring at the remote-node node and not at the node reporting the FE-LOCKOUTOFPR-SPAN condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-LOCKOUTOFPR-SPAN Condition

-
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Ensure there is no lockout set. Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-267.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.112 FE-LOF

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End LOF condition occurs when a remote node reports the “[LOF \(DS3\)](#)” alarm on page 2-141 in C-bit framing mode.

The prefix FE in an alarm or condition occurs when the main alarm is occurring at the remote-node node and not at the node reporting the FE-LOF condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-LOF Condition

-
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Complete the [“Clear the LOF \(DS1\) Alarm” procedure on page 2-141](#). It also applies to FE-LOF.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.113 FE-LOS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The Far End LOS condition occurs in C-bit framing mode when a remote node reports the [“LOS \(DS3\)” alarm on page 2-149](#).

The prefix FE occurs when the main alarm is occurring at the remote-node node, and not at the node reporting the FE-LOS condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-LOS Condition

-
- Step 1** To troubleshoot the FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Complete the [“Clear the LOS \(DS1\) Alarm” procedure on page 2-148](#).
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.114 FE-MANWKSWBK-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Manual Switch Back to Working—Span condition occurs when a remote-node path protection span is Manual switched back to working.

**Note**

WKSWBK-type conditions apply only to nonrevertive circuits.

The prefix FE occurs when the main alarm is occurring at the remote-node node, and not at the node reporting the FE-LOS condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-MANWKSWBK-SPAN Condition

-
- Step 1** To troubleshoot the FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.
 - Step 2** Log into the node that links directly to the card reporting the FE condition.
 - Step 3** Complete the [“Clear a BLSR External Switching Command” procedure on page 2-267](#).
 - Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.115 FE-MANWKSWPR-RING

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Ring Manual Switch of Working Facility to Protect condition occurs when a BLSR working ring is switched from working to protect at a remote-node node using the Manual Ring command.

The prefix FE means the main alarm is occurring at the remote-node node and not at the node reporting the FE-MANWKSWPR-RING condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-MANWKSWPR-RING Condition

-
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.
 - Step 2** Log into the node that links directly to the card reporting the FE condition.
 - Step 3** Complete the [“Clear a BLSR External Switching Command” procedure on page 2-267](#).
 - Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.116 FE-MANWKSWPR-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far-End Span Manual Switch Working Facility to Protect condition occurs when a four-fiber BLSR span is switched from working to protect at the remote-node node using the Manual to Protect command.

The prefix FE means the main alarm is occurring at the remote-node node and not at the node reporting the alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-MANWKSWPR-SPAN Condition

-
- Step 1** To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Complete the [“Clear a BLSR External Switching Command” alarm on page 2-267](#).
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.117 FEPRLF

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Far End Protection Line Failure alarm occurs when an APS channel [“SF \(DS1, DS3\)” condition on page 2-221](#) occurs on the protect card coming into the node.

**Note**

The FEPRLF alarm occurs when bidirectional protection is used on optical cards in a 1+1 configuration or four-fiber BLSR configuration.

Clear the FEPRLF Alarm on a Four-Fiber BLSR

-
- Step 1** To troubleshoot the FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.
- Step 2** Log into the node that links directly to the card reporting the FE condition.
- Step 3** Clear the main alarm. Refer to the appropriate alarm section in this chapter in this chapter for instructions.

- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.118 FIBERTEMP-DEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Fiber Temperature Degrade alarm occurs when a DWDM card internal heater-control circuit fails. Degraded temperature can cause some signal drift. The card should be replaced at the next opportunity.

Clear the FIBERTEMP-DEG Alarm

- Step 1** For the alarmed card, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) at the next opportunity.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.119 FORCED-REQ

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EQPT, STSMON, VT-MON

The Force Switch Request on Facility or Port condition occurs when you enter the Force command on a port to force traffic from a working port to a protect port or protection span (or vice versa). You do not need to clear the condition if you want the Force switch to remain.

Clear the FORCED-REQ Condition

- Step 1** Complete the [“Clear a 1+1 Protection Port Force or Manual Switch Command” procedure on page 2-261](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.120 FORCED-REQ-RING

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Force Switch Request Ring condition applies to optical trunk cards when the Force Ring command is applied to two-fiber and four-fiber BLSRs to move traffic from working to protect.

Clear the FORCED-REQ-RING Condition

-
- Step 1** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-267.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.121 FORCED-REQ-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, TRUNK

The Force Switch Request Span condition applies to optical trunk cards in two-fiber or four-fiber BLSRs when the Force Span command is applied to a BLSR to force traffic from working to protect or from protect to working.

Clear the FORCED-REQ-SPAN Condition

-
- Step 1** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-267.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.122 FRCDSWTOINT

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE-SREF

The Force Switch to Internal Timing condition occurs when the user issues a Force command to switch to an internal timing source.



Note FRCDSWTOINT is an informational condition and does not require troubleshooting.

2.8.123 FRCDSWTOPRI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Primary Timing Source condition occurs when the user issues a Force command to switch to the primary timing source.



Note FRCDSWTOPRI is an informational condition and does not require troubleshooting.

2.8.124 FRCDSWTOSEC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Second Timing Source condition occurs when the user issues a Force command to switch to the second timing source.



Note

FRCDSWTOSEC is an informational condition and does not require troubleshooting.

2.8.125 FRCDSWTOTHIRD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Third Timing Source condition occurs when the user issues a Force command to switch to the third timing source.



Note

FRCDSWTOTHIRD is an informational condition and does not require troubleshooting.

2.8.126 FRNGSYNC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE-SREF

The Free Running Synchronization Mode condition occurs when the reporting ONS 15454 is in free-run synchronization mode. External timing sources have been disabled and the node is using its internal clock, or the node has lost its designated building integrated timing supply (BITS) timing source. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS 15454 node relying on an internal clock.



Note

If the ONS 15454 is configured to operate from its internal clock, disregard the FRNGSYNC condition.

Clear the FRNGSYNC Condition

-
- Step 1** If the ONS 15454 is configured to operate from an external timing source, verify that the BITS timing source is valid. Common problems with a BITS timing source include reversed wiring and bad timing cards. Refer to the *<I_Ital>Cisco ONS 15454 Reference Manual* for more information about timing.
- Step 2** If the BITS source is valid, clear alarms related to the failures of the primary and secondary reference sources, such as the “[SYNCPRI](#)” alarm on page 2-239 and the “[SYNCSEC](#)” alarm on page 2-240.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.127 FSTSYNC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE-SREF

A Fast Start Synchronization mode alarm occurs when the node is choosing a new timing reference. The previous timing reference has failed.

The FSTSYNC alarm disappears after approximately 30 seconds. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

**Note**

FSTSYNC is an informational alarm. It does not require troubleshooting.

2.8.128 FULLPASSTHR-BI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Bidirectional Full Pass-Through Active condition occurs on a nonswitching node in a BLSR when the protect channels on the node are active and carrying traffic and there is a change in the receive K byte from No Request.

Clear the FULLPASSTHR-BI Condition

-
- Step 1** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-267.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.129 GAIN-HDEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Gain High Degrade alarm is raised on DWDM OPT-BST and OPT-PRE amplifier cards when the gain reaches the high degrade threshold and is prevented from reaching the setpoint due to an internal failure. The card should be replaced at the first opportunity.

**Note**

This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-HDEG Alarm

-
- Step 1** Verify fiber continuity to the port.



Note To verify fiber continuity, follow site practices.

- Step 2** If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.
- Step 3** Verify that the received power (opwrMin) is within the expected range shown in Cisco MetroPlanner. To check the level in CTC:
- Double-click the amplifier card to display the card view.
 - Display the optical thresholds by clicking the OPT-BST or OPT-PRE **Provisioning > Opt. Ampli. Line > Optics Thresholds** tab.
- Step 4** If the power value is outside the expected range, verify that all impacted optical signal sources are in IS-NR service state and that their outputs are within expected range. Optical signal sources include the trunk port of a TXP or MXP card, or an ITU-T line card.
- Step 5** If the signal source is OOS,DSBLD admin state, put it in IS state. This creates the IS-NR service state.
- Step 6** If the service state is IS-NR but the output power is outside of specifications, complete the [“Clear the LOS-P \(OCH\) Alarm” procedure on page 2-159](#).
- Step 7** If the signal source is IS and the power is within the expected range, go back to the unit reporting the alarm and clean the fiber connected to amplifier's COM-RX port according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”



Note Unplugging fiber from the COM-RX port can cause a traffic hit. To avoid this, perform a traffic switch if possible using the procedures outlined in the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#). For more in-depth information about protection switches, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

- Step 8** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem. To do this, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for acceptance testing procedures that can be used for troubleshooting purposes.
- Step 9** If no other alarms exist that could be the source of the GAIN-HDEG, or if clearing an alarm did not clear the GAIN-HDEG, place all of the card ports in OOS,DSBLD admin state.
- Step 10** Complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the reporting card.



Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform a traffic switch if possible.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database apart from restoring the card's port to the IS,AINS admin state.

- Step 11** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.130 GAIN-HFAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: AOTS

The Gain High Fail alarm is raised on DWDM OPT-BST and OPT-PRE amplifier cards when the gain crosses the high failure point threshold. The card must be replaced.



Note

This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-HFAIL Alarm

-
- Step 1** For the alarmed card, complete the “[Clear the GAIN-HDEG Alarm](#)” procedure on page 2-113.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.8.131 GAIN-LDEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Gain Low Degrade alarm is raised on DWDM OPT-BST and OPT-PRE amplifier cards when the gain has crossed the low degrade threshold and is prevented from reaching the setpoint due to an internal failure. The card should be replaced at the first opportunity.



Note

This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-LDEG Alarm

-
- Step 1** For the alarmed card, complete the “[Clear the GAIN-HDEG Alarm](#)” procedure on page 2-113.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.132 GAIN-LFAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: AOTS

The Gain Low Fail alarm is raised on DWDM OPT-BST and OPT-PRE amplifier cards when the gain crosses the low failure point threshold. The card must be replaced.

**Note**

This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-LFAIL Alarm

-
- Step 1** For the alarmed card, complete the “[Clear the GAIN-HDEG Alarm](#)” procedure on page 2-113.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.133 GCC-EOC

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The GCC Embedded Operation Channel Failure alarm applies to the optical transport network (OTN) communication channel for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. The GCC-EOC is raised when the channel cannot operate.

Clear the GCC-EOC Alarm

-
- Step 1** Complete the “[Clear the EOC Alarm](#)” procedure on page 2-79.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.134 GE-OOSYNC

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: FC, GE, ISC, TRUNK

The Gigabit Ethernet Out of Synchronization alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, and TXPP_MR_2.5G cards when the Gigabit Ethernet signal is out of synchronization and is very similar to the SONET LOS alarm. This alarm can occur when you try to input a SONET signal to the TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card. A signal is present, so there is no CARLOSS alarm, but it is not correctly formatted for the card and so raises the GE-OOSYNC alarm.

Clear the GE-OOSYNC Alarm

-
- Step 1** Ensure that the incoming signal is provisioned with the correct physical-layer protocol.
- Step 2** Ensure that the line is provisioned with the correct line speed (10 Gbps).
-

- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.135 GFP-CSF

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: CE100T, FCMR, GFP-FAC, ML100T, ML1000

The GFP Client Signal Fail Detected alarm is a secondary alarm raised on local GFP data ports when a service-affecting alarm such as the “SIGLOSS” alarm on page 2-225, an Ethernet client loss [2.8.46 CARLOSS (CE100T), 2.8.47 CARLOSS (E100T, E1000F), 2.8.46 CARLOSS (CE100T), or 2.8.50 CARLOSS (G1000), 2.8.49 CARLOSS (FC), 2.8.51 CARLOSS (GE), 2.8.52 CARLOSS (ISC)], a trunk carrier loss (the “CARLOSS (TRUNK)” alarm on page 2-63), or a 2.8.345 SYNCLOSS alarm causes invalid data transmission. The alarm is raised locally on FC_MR-4, ML100T, ML1000, MXP_MR_25G, MXPP_MR_25G, TXP, or TXPP data ports and indicates that a signal loss or frame failure (such as from a degraded or pulled Rx cable) has affected a remote data port's Rx. This alarm can be demoted when a facility loopback is placed on the FC_MR-4 port.

Clear the GFP-CSF Alarm

- Step 1** Clear the service-affecting alarm at the remote data port, using the appropriate procedure in this chapter.
- Step 2** If the GFP-CSF alarm does not also clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.8.136 GFP-DE-MISMATCH

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: FCMR, GFP-FAC, ML100T, ML1000

The GFP Fibre Channel Distance Extension Mismatch alarm indicates that a port configured for Distance Extension is connected to a port that is not operating in Cisco's proprietary Distance Extension mode. It is raised on Fibre Channel and FICON card GFP ports supporting distance extension. The alarm occurs when distance extension is enabled on one side of the transport but not on the other. To clear, distance extension must be enabled on both ports connected by a circuit.

Clear the GFP-DE-MISMATCH Alarm

- Step 1** Ensure that the distance extension protocol is configured correctly on both sides:
- a. Double-click the card to display the card view.
 - b. Click the **Provisioning > Port > General** tabs.
 - c. Under Admin State, click the cell and choose **OOS,MT**.
 - d. Click **Apply**.

- e. Click the **Provisioning > Port > Distance Extension** tabs.
- f. Check the check box in the **Enable Distance Extension** column.
- g. Click **Apply**.
- h. Click the **Provisioning > Port > General** tabs.
- i. Under Admin State, click the cell and choose **IS-NR**.
- j. Click **Apply**.

Step 2 If the GFP-DE-MISMATCH alarm does not also clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service affecting problem.

2.8.137 GFP-EX-MISMATCH

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: FCMR, GFP-FAC, ML100T, ML1000

The GFP Extension Header Mismatch alarm is raised on Fibre Channel/FICON cards when it receives frames with an extension header that is not null. The alarm occurs when a provisioning error causes all GFP frames to be dropped for 2.5 seconds.

Ensure that both end ports are sending a null extension header for a GFP frame. The FC_MR-4 card always sends a null extension header, so if the equipment is connected to other vendors' equipment, those need to be provisioned appropriately.

Clear the GFP-EX-MISMATCH Alarm

- Step 1** Ensure that the vendor equipment is provisioned to send a null extension header in order to interoperate with the FC_MR-4 card. (The FC_MR-4 card always sends a null extension header.)
 - Step 2** If the GFP-EX-MISMATCH alarm does not also clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service affecting problem.
-

2.8.138 GFP-LFD

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: CE100T, FCMR, GFP-FAC, ML100T, ML1000

The GFP Loss of Frame Delineation alarm applies to Fibre Channel/FICON GFP ports and occurs if there is a bad SONET connection, if SONET path errors cause GFP header errors in the check sum calculated over payload length (PLI/cHEC) combination, or if the GFP source port sends an invalid PLI/cHEC combination. The loss causes traffic stoppage.

Clear the GFP-LFD Alarm

-
- Step 1** Look for and clear any associated SONET path errors such as LOS or AIS-L originating at the transmit node.
- Step 2** If the GFP-LFD alarm does not also clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service affecting problem.
-

2.8.139 GFP-NO-BUFFERS

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: FCMR, GFP-FAC, ML100T, ML1000

The GFP Fibre Channel Distance Extension Buffer Starvation alarm is raised on Fibre Channel/FICON card ports supporting GFP and the distance extension protocol when the GFP transmitter cannot send GFP frames due to lack of remote GFP receiver buffers. This occurs when the remote GFP-T receiver experiences congestion and is unable to send frames over the Fibre Channel/FICON link.

This alarm might be raised in conjunction with the FC-NO-CREDITS alarm. For example, if the FC-NO-CREDITS alarm is generated at an FC_MR-4 data port, a GFP-NO-BUFFERS alarm might be raised at the upstream remote FC_MR-4 data port.

Clear the GFP-NO-BUFFERS Alarm

-
- Step 1** Complete the “[Clear the FC-NO-CREDITS Alarm](#)” procedure on page 2-98.
- Step 2** If the GFP-NO-BUFFERS alarm does not also clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service affecting problem.
-

2.8.140 GFP-UP-MISMATCH

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: FCMR, GFP-FAC, ML100T, ML1000

The GFP User Payload Mismatch is raised against Fibre Channel/FICON ports supporting GFP. It occurs when the received frame user payload identifier (UPI) does not match the transmitted UPI and all frames are dropped. The alarm is caused by a provisioning error, such as the port media type not matching the remote port media type. For example, the local port media type could be set to Fibre Channel 1 Gig or Fibre Channel 2 Gig and the remote port media type could be set to FICON 1 Gig or FICON 2 Gig.

Clear the GFP-UP-MISMATCH Alarm

-
- Step 1** Ensure that the transmit port and receive port are provisioned the same way for distance extension:
- Double-click the card to display the card view.
 - Click the **Provisioning > Port > Distance Extension** tabs.
 - Check the check box in the **Enable Distance Extension** column.
 - Click **Apply**.
- Step 2** Ensure that both ports are set for the correct media type. For each port, complete the following:
- Double-click the card to display the card view (if you are not already in card view).
 - Click the **Provisioning > Port > General** tabs.
 - Choose the correct media type (Fibre Channel 1 Gbps, Fibre Channel 2 Gbps, FICON 1 Gbps, or FICON 2 Gbps) from the drop-down list.
 - Click **Apply**.
- Step 3** If the GFP-UP-MISMATCH alarm does not also clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service affecting problem.
-

2.8.141 HELLO

- Default Severity: Minor (MN), Non-Service-Affecting (NSA)
- Logical Objects: OCN

The Open Shortest Path First (OSPF) Hello alarm is raised when the two end nodes cannot bring an OSPF neighbor up to the full state. Typically, this problem is caused by an area ID mismatch, and/or an OSPF HELLO packet loss over the DCC.

Clear the HELLO Alarm

-
- Step 1** Ensure that the area ID is correct on the missing neighbor:
- In node view, click the **Provisioning > Network > OSPF** tabs.
 - Ensure that the IP address in the Area ID column matches the other nodes.
 - If the address does not match, click the incorrect cell and correct it.
 - Click **Apply**.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.142 HIBATVG

- Default Severity: Major (MJ), Service-Affecting (SA)

- Logical Object: PWR

The High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the high power threshold. This threshold, with a default value of –52 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds. (For information about changing this threshold, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 4, “Turn Up Node.”)

Clear the HIBATVG Alarm

-
- Step 1** The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.143 HI-CCVOLT

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: BITS

The 64K Composite Clock High NE Voltage alarm occurs when the 64K signal peak voltage exceeds 1.1 Vdc.

Clear the HI-CCVOLT Condition

-
- Step 1** Lower the source voltage to the clock.
- Step 2** If the condition does not clear, add more cable length or add a 5 dBm attenuator to the cable.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.144 HI-LASERBIAS

- Default Severity: Minor (MN), Non-Service Affecting (NSA) for 2R, ESCON, FC, GE, ISC, OCN, TRUNK; Not Alarmed (NA), Non-Service Affecting (NSA) for PPM
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, PPM, TRUNK

The Equipment High Transmit Laser Bias Current alarm is raised against TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G card laser performance. The alarm indicates that the card laser has reached the maximum laser bias tolerance.

Laser bias typically starts at about 30 percent of the manufacturer maximum laser bias specification and increases as the laser ages. If the HI-LASERBIAS alarm threshold is set at 100 percent of the maximum, the laser usability has ended. If the threshold is set at 90 percent of the maximum, the card is still usable for several weeks or months before it needs to be replaced.

Clear the HI-LASERBIAS Alarm

Step 1 Complete the [“Clear the LASEREOL Alarm” procedure on page 2-135](#). Replacement is not urgent and can be scheduled during a maintenance window.



Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 2 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.145 HI-LASERTEMP

- Default Severity: Minor (MN), Non-Service Affecting (NSA) or OCN; Not Alarmed (NA), Non-Service Affecting (NSA) for PPM
- Logical Objects: OCN, PPM

The Equipment High Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. HI-LASERTEMP occurs when the internally measured transceiver temperature exceeds the card setting by 35.6 degrees F (2 degrees C). A laser temperature change affects the transmitted wavelength.

When the TXP or MXP card raises this alarm, the laser is automatically shut off. The [“LOS \(OCN\)” alarm on page 2-153](#) is raised at the remote node and the [“DSP-FAIL” alarm on page 2-75](#) is raised at the local node.

Clear the HI-LASERTEMP Alarm

Step 1 In node view, double-click the card to display the card view.

Step 2 Click the **Performance > Optics PM** tabs.

Step 3 Verify the card laser temperature levels. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Step 4 Complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for the reporting MXP or TXP card.

Step 5 If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the reporting MXP or TXP card.

Step 6 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.146 HI-RXPOWER

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, TRUNK

The Equipment High Receive Power alarm is an indicator of the optical signal power that is transmitted to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, or MXP_2.5G_10G card. HI-RXPOWER occurs when the measured optical power of the received signal exceeds the threshold. The threshold value is user-provisionable.

Clear the HI-RXPOWER Alarm

Step 1 Find out whether gain (the amplification power) of any amplifiers has been changed. This change also causes channel power to need adjustment.

Step 2 Find out whether channels have been dropped from the fiber. Increasing or decreasing channels can affect power. If channels have been dropped, the power levels of all channels have to be adjusted.



Note If the card is part of an amplified DWDM system, dropping channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

Step 3 At the transmit end of the errored circuit, decrease the transmit power level within safe limits.

Step 4 If neither of these problems cause the HI-RXPOWER alarm, there is a slight possibility that another wavelength is drifting on top of the alarmed signal. In this case, the receiver gets signals from two transmitters at the same time and data alarms would be present. If wavelengths are drifting, the data is garbled and receive power increases by about +3 dBm.

Step 5 If the alarm does not clear, add fiber attenuators to the receive ports. Start with low-resistance attenuators and use stronger ones as needed, depending on factors such as the transmission distance, according to standard practice.

Step 6 If the alarm does not clear and no faults are present on the other port(s) of the transmit or receive card, use a known-good loopback cable to complete the [“1.6.1 Perform a Facility \(Line\) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port” procedure on page 1-88](#) and test the loopback.

Step 7 If a port is bad and you need to use all the port bandwidth, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#). If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 8 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.147 HITEMP

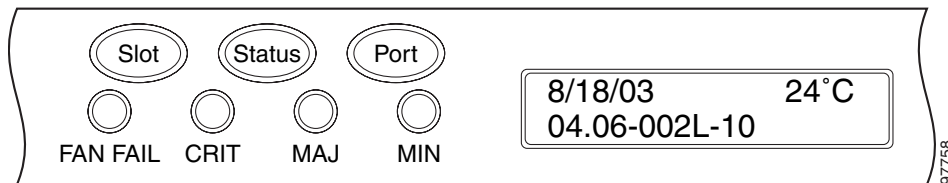
- Default Severity: Critical (CR), Service-Affecting (SA) for NE; Default Severity: Minor (MN), Non-Service Affecting (NSA) for EQPT
- Logical Objects: EQPT, NE

The High Temperature alarm occurs when the temperature of the ONS 15454 is above 122 degrees F (50 degrees C).

Clear the HITEMP Alarm

- Step 1** View the temperature displayed on the ONS 15454 LCD front panel ([Figure 2-2](#)).

Figure 2-2 Shelf LCD Panel



- Step 2** Verify that the environmental temperature of the room is not abnormally high.
- Step 3** If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15454 shelf.
- Step 4** If airflow is not blocked, physically ensure that blank faceplates fill the ONS 15454 shelf empty slots. Blank faceplates help airflow.
- Step 5** If faceplates fill the empty slots, determine whether the air filter needs replacement. Refer to the [“Inspect, Clean, and Replace the Reusable Air Filter”](#) procedure on page 2-275.



Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 6** If the fan does not run or the alarm persists, complete the [“Replace the Fan-Tray Assembly”](#) procedure on page 2-277.



Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.



Note The fan should run immediately when correctly inserted.

- Step 7** If the replacement fan-tray assembly does not operate correctly, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447) if it applies to the NE, or a non-service-affecting problem if it applies to equipment.
-

2.8.148 HI-TXPOWER

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, PPM, TRUNK

The Equipment High Transmit Power alarm is an indicator on the TXP_MR_E, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card transmitted optical signal power. HI-TXPOWER occurs when the measured optical power of the transmitted signal exceeds the threshold.

Clear the HI-TXPOWER Alarm

- Step 1** In node view, display the card view for the TXP_MR_E, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card.
- Step 2** Click the **Provisioning > Optical Thresholds** tabs.
- Step 3** Decrease (change toward the negative direction) the OPT-HIGH column value by 0.5 dBm.
- Step 4** If the card transmit power setting cannot be lowered without disrupting the signal, complete the [“Physically Replace a Traffic Card”](#) section on page 2-271.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing”](#) section on page 2-260 for commonly used traffic-switching procedures.



Note

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.149 HLDVRSYNC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE-SREF

The Holdover Synchronization Mode condition indicates a loss of the primary or secondary timing reference. Timing reference loss occurs when line coding on the timing input is different from the configuration on the ONS 15454. It also usually occurs during the selection of a new node reference

clock. The HLDOVRSYNC condition indicates that the ONS 15454 has gone into holdover and is using the ONS node internal reference clock, which is a Stratum 3-level timing device. The condition clears when primary or secondary timing is reestablished.

Clear the HLDOVRSYNC Condition

-
- Step 1** Clear additional alarms that relate to timing, such as:
- 2.8.126 FRNGSYNC, page 2-112
 - 2.8.127 FSTSYNC, page 2-113
 - 2.8.149 HLDOVRSYNC, page 2-125
 - 2.8.173 LOF (BITS), page 2-139
 - 2.8.185 LOS (BITS), page 2-147
 - 2.8.231 MANSWTOINT, page 2-177
 - 2.8.232 MANSWTOPRI, page 2-178
 - 2.8.233 MANSWTOSEC, page 2-178
 - 2.8.234 MANSWTOTHIRD, page 2-178
 - 2.8.341 SWTOPRI, page 2-237
 - 2.8.342 SWTOSEC, page 2-237
 - 2.8.343 SWTOTHIRD, page 2-237
 - 2.8.344 SYNC-FREQ, page 2-238
 - 2.8.346 SYNCPRI, page 2-239
 - 2.8.347 SYNCSEC, page 2-240
 - 2.8.348 SYNCTHIRD, page 2-240
- Step 2** Reestablish a primary and secondary timing source according to local site practice. If none exists, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 10, “Change Node Settings.”
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.150 I-HITEMP

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: NE

The Industrial High Temperature alarm occurs when the temperature of the ONS 15454 is above 149 degrees F (65 degrees C) or below –40 degrees F (–40 degrees C). This alarm is similar to the HITEMP alarm but is used for the industrial environment. If this alarm is used, you can customize your alarm profile to ignore the lower-temperature HITEMP alarm.

Clear the I-HITEMP Alarm

-
- Step 1** Complete the “[Clear the HITEMP Alarm](#)” procedure on page 2-124.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call TAC (1-800-553-2447) in order to report a service-affecting problem.
-

2.8.151 IMPROPRMVL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: EQPT, PPM

The Improper Removal equipment alarm occurs when a card is physically removed from its slot before it is deleted from CTC. The card does not need to be in service to cause the IMPROPRMVL alarm; it only needs to be recognized by CTC. The alarm does not appear if you delete the card from CTC before you physically remove the card from the node. It can also occur if the card is inserted into a slot but is not fully plugged into the backplane. For PPMs, the alarm occurs if you provision a PPM but no physical module is inserted on the port.



Caution

Do not remove a card during a card reboot. If CTC begins to reboot a card before you remove the card, allow the card to finish rebooting. After the card reboots, delete the card in CTC again and physically remove the card before it begins to reboot. When you delete the card, CTC loses connection with the node view and go to network view.



Note

CTC gives the user approximately 15 seconds to physically remove the card before CTC begins a card reboot.



Note

It can take up to 30 minutes for software to be updated on a standby TCC2/TCC2P card.

Clear the IMPROPRMVL Alarm

-
- Step 1** In node view, right-click the card reporting the IMPROPRMVL.
- Step 2** Choose **Delete** from the shortcut menu.



Note

CTC does not allow you to delete the reporting card if the card is in service, has a circuit mapped to it, is paired in a working protection scheme, has DCC enabled, or is used as a timing reference.

- Step 3** If any ports on the card are in service, place them out of service (OOS,MT):



Caution

Before placing a port out of service (OOS,MT or OOS,DSBLD), ensure that no live traffic is present.

- In node view, double-click the reporting card to display the card view.

- b. Click the **Provisioning > Line** tab.
- c. Click the Admin State column of any in-service (IS) ports.
- d. Choose **OOS,MT** to take the ports out of service.

Step 4 If a circuit has been mapped to the card, complete the “Delete a Circuit” procedure on page 2-272.

**Caution**

Before deleting the circuit, ensure that the circuit does not carry live traffic.

Step 5 If the card is paired in a protection scheme, delete the protection group:

- a. Click **View > Go to Previous View** to return to node view.
- b. If you are already in node view, click the **Provisioning > Protection** tabs.
- c. Click the protection group of the reporting card.
- d. Click **Delete**.

Step 6 If the card is provisioned for DCC, delete the DCC provisioning:

- a. Click the ONS 15454 **Provisioning > Comm Channels > SDCC** tabs.
- b. Click the slots and ports listed in DCC terminations.
- c. Click **Delete** and click **Yes** in the dialog box that appears.

Step 7 If the card is used as a timing reference, change the timing reference:

- a. Click the **Provisioning > Timing** tabs.
- b. Under NE Reference, click the drop-down arrow for **Ref-1**.
- c. Change Ref-1 from the listed OC-N card to **Internal Clock**.
- d. Click **Apply**.

Step 8 Right-click the card reporting the IMPROPRMVL alarm and choose **Delete**.

Step 9 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.152 INC-ISD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The DS-3 Idle condition indicates that the DS-3 card is receiving an idle signal, meaning that the payload of the signal contains a repeating pattern of bits. The INC-ISD condition occurs when the transmitting port has an OOS-MA,MT service state. It is resolved when the OOS-MA,MT state ends.

**Note**

INC-ISD is a condition and not an alarm. It is for information only and does not require troubleshooting.

2.8.153 INHSWPR

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: EQPT

The Inhibit Switch To Protect Request on Equipment condition occurs on traffic cards when the ability to switch to protect has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the working system. If the card is part of a 1:N protection scheme, traffic can be switched between working cards when the switch to protect is disabled.

Clear the INHSWPR Condition

-
- Step 1** If the condition is raised against a 1+1 port, complete the “[Initiate a 1+1 Protection Port Manual Switch Command](#)” section on page 2-261.
- Step 2** If it is raised against a 1:1 card, complete the “[Initiate a 1:1 Card Switch Command](#)” procedure on page 2-263 to switch it back.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.154 INHSWWKG

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Inhibit Switch To Working Request on Equipment condition occurs on traffic cards when the ability to switch to working has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the protect system. If the card is part of a 1:N protection scheme, traffic can be switched between protect cards when the switch to working is disabled.

Clear the INHSWWKG Condition

-
- Step 1** If the condition is raised against a 1+1 port, complete the “[Initiate a 1+1 Protection Port Manual Switch Command](#)” section on page 2-261.
- Step 2** If it is raised against a 1:1 card, complete the “[Initiate a 1:1 Card Switch Command](#)” procedure on page 2-263 to switch traffic back.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.155 INTRUSION-PSWD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The Security Intrusion Incorrect Password condition occurs after a user attempts a provisionable (by Superuser) number of unsuccessful logins, a login with an expired password, or an invalid password. The alarmed user is locked out of the system, and INTRUSION-PSWD condition is raised. The INTRUSION-PSWD condition is automatically cleared when a provisionable lockout timeout expires, or it can be manually cleared in CTC by the Superuser if lockout is permanent.

**Note**

This condition is only shown in Superuser login sessions, not login sessions for lower-level users.

Clear the INTRUSION-PSWD Condition

-
- Step 1** In node view, click the **Provisioning > Security** tabs.
- Step 2** Click the **Clear security intrusion alarm** button.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.156 INVMACADR

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: AIP, BPLANE

The Equipment Failure Invalid Media Access Control (MAC) Address alarm occurs when the ONS 15454 MAC address is invalid. Each ONS 15454 has a unique, permanently assigned MAC address. The address resides on an AIP EEPROM. The TCC2/TCC2P card reads the address value from the AIP chip during boot-up and keeps this value in its synchronous dynamic RAM (SDRAM).

Under normal circumstances, the read-only MAC address can be viewed in the Provisioning/Network tab in CTC.

The ONS 15454 uses both IP and MAC addresses for circuit routing. When an INVMACADR alarm exists on a node, you see a PARTIAL circuit in the CTC circuit status column. The circuit works and is able to carry traffic, but CTC cannot logically display the circuit end-to-end information.

An invalid MAC address can be caused when:

- There is a read error from the AIP during bootup; in this case, the reading TCC2/TCC2P uses the default MAC address (00-10-cf-ff-ff-ff).
- There is a read error occurring on one of the redundant TCC2/TCC2P cards that read the address from the AIP; these cards read the address independently and could therefore each read different address values.
- An AIP component failure causes a read error.
- The ribbon cable connecting the AIP card to the backplane is bad.

Clear the INVMACADR Alarm

-
- Step 1** Check for any outstanding alarms that were raised against the active and standby TCC2/TCC2P and resolve them.

Step 2 If the alarm does not clear, determine whether the LCD display on the fan tray ([Figure 2-2 on page 2-124](#)) is blank or if the text is garbled. If so, proceed to [Step 8](#). If not, continue with [Step 3](#).

Step 3 At the earliest maintenance window, reset the standby TCC2/TCC2P:



Note The reset requires approximately five minutes. Do not perform any other step until the reset is complete.

- a. Log into a node on the network. If you are already logged in, continue with [Step b](#).
- b. Identify the active TCC2/TCC2P card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- c. Right-click the standby TCC2/TCC2P card in CTC.
- d. Choose **Reset Card** from the shortcut menu.
- e. Click **Yes** in the Are You Sure dialog box.
The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.
- f. Verify that the reset is complete and error-free, and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- g. Double-click the node and ensure that the reset TCC2/TCC2P card is still in standby mode and that the other TCC2/TCC2P card is active.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- h. Ensure that no new alarms associated with this reset appear in the CTC Alarms window.

If the standby TCC2/TCC2P fails to boot into standby mode and reloads continuously, the AIP is probably defective. In this case, the standby TCC2/TCC2P is unsuccessfully attempting to read the EEPROM located on the AIP. The TCC2/TCC2P reloads until it reads the EEPROM. Proceed to [Step 8](#).

Step 4 If the standby TCC2/TCC2P rebooted successfully into standby mode, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-270](#).

Resetting the active TCC2/TCC2P causes the standby TCC2/TCC2P to become active. The standby TCC2/TCC2P keeps a copy of the chassis MAC address. If its stored MAC address is valid, the alarm should clear.

Step 5 After the reset, note whether or not the INVMACADR alarm has cleared or is still present.

Step 6 Complete the [“Reset an Active TCC2/TCC2P and Activate the Standby Card” procedure on page 2-268](#) again to place the standby TCC2/TCC2P back into active mode.

After the reset, note whether or not the INVMACADR alarm has cleared or is still present. If the INVMACADR alarm remains standing through both TCC2/TCC2P resets, this indicates that the AIP is probably defective. Proceed to [Step 8](#).

If the INVMACADR was raised during one TCC2/TCC2P reset and cleared during the other, the TCC2/TCC2P that was active while the alarm was raised needs to be replaced. Continue with [Step 7](#).

Step 7 If the faulty TCC2/TCC2P is currently in standby mode, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for this card. If the faulty TCC2/TCC2P card is currently active, during the next available maintenance window complete the [“Reset an Active TCC2/TCC2P and Activate the Standby Card” procedure on page 2-268](#) and then complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#).



Note If the replacement TCC2/TCC2P is loaded with a different software version from the current TCC2/TCC2P card, the card bootup might take up to 30 minutes. During this time, the card LEDs flicker between Fail and Act/Sby as the active TCC2/TCC2P version software is copied to the new standby card.

- Step 8** Open a case with Cisco TAC (1 800 553-2447) for assistance with determining the node's previous MAC address.
- Step 9** Replace the ribbon cable between the system board and the AIP with a known-good cable.
- Step 10** If the alarm persists, complete the [“Replace the Alarm Interface Panel” procedure on page 2-279](#).
- Step 11** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.157 IOSCFGCOPY

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The IOS Configuration Copy in Progress condition occurs on ML-Series Ethernet cards when a Cisco IOS startup configuration file is being uploaded or downloaded to or from an ML-Series card. (This condition is very similar to the [“SFTWDOWN” condition on page 2-224](#) but it applies to ML-Series Ethernet cards rather than to the TCC2/TCC2P.)

The condition clears after the copy operation is complete. (If it does not complete correctly, the [“NO-CONFIG” condition on page 2-186](#) might be raised.)



Note IOSCFGCOPY is an informational condition.



Note For more information about the ML-Series Ethernet cards, refer to the *<I Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

2.8.158 KB-PASSTHR

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The K Bytes Pass Through Active condition occurs on a nonswitching node in a BLSR when the protect channels on the node are not active and the node is in K Byte pass-through state. It also occurs when a BLSR ring is being exercised using the Exercise Ring command.

Clear the KB-PASSTHR Condition

-
- Step 1** Complete the [“Clear a BLSR External Switching Command” procedure on page 2-267](#).

- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.159 KBYTE-APS-CHANNEL-FAILURE

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The APS Channel Failure alarm is raised when a span is provisioned for different APS channels on each side. For instance, the alarm is raised if K3 is selected on one end and F1, E2, or Z2 is selected on the other end.

This alarm is also raised during checksum failure if the K1 and K2 bytes are overwritten by test equipment. It is not raised in bidirectional full pass-through or K-byte pass-through states. The alarm is overridden by [2.8.3 AIS-P, page 2-31](#), [2.8.177 LOF \(OCN\), page 2-143](#), [2.8.193 LOS \(OCN\), page 2-153](#) or [2.8.311 SF-P, page 2-223](#).

Clear the KBYTE-APS-CHANNEL-FAILURE Alarm

- Step 1** The alarm is most frequently raised due to mismatched span provisioning. In this case, reprovision one side of the span with the same parameters. To do this, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 5, “Turn Up Network.”
- Step 2** If the error is not caused by misprovisioning, it is due to checksum errors within an OC-N, cross-connect, or TCC2/TCC2P card. In this case, complete the [“Side Switch the Active and Standby XC10G Cross-Connect Cards” procedure on page 2-269](#) to allow CTC to resolve the issue.
- Step 3** If third-party equipment is involved, ensure that it is configured for the same APS channel as the Cisco ONS equipment.
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.160 LAN-POL-REV

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

The LAN Connection Polarity Reversed condition is not raised in shelves that contain TCC2 cards. It is raised during software upgrade when the card detects that a connected Ethernet cable has reversed receive wire pairs. The card automatically compensates for this reversal, but LAN-POL-REV stays active.

Clear the LAN-POL-REV Condition

- Step 1** Replace the connected Ethernet cable with a cable that has the correct pinout. For correct pin mapping, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.161 LASER-APR

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Laser Automatic Power Reduction (APR) alarm condition is raised by OSC-CSM, OSCM, OPT-BST, and OPT-PRE cards when the laser is working in power reduction mode. The condition clears as soon as safety conditions are released and the power value reaches the normal setpoint.

**Note**

LASER-APR is an informational condition and does not require troubleshooting.

2.8.162 LASERBIAS-DEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OTS

The Laser Bias Current Degrade alarm occurs on DWDM amplifier cards such as the OPT-BST or OPT-PRE when laser aging causes a degrade, but not failure, of laser transmission. The card should be replaced at the next opportunity.

Clear the LASERBIAS-DEG Alarm

- Step 1** For the alarmed card, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) at the next opportunity.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.163 LASERBIAS-FAIL

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Laser Bias Current Failure alarm occurs on DWDM amplifier cards such as OPT-BST or OPT-PRE when the laser control circuit fails or if the laser itself fails service. The card must be replaced to restore traffic.

Clear the LASERBIAS-FAIL Alarm

- Step 1** For the alarmed card, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#).

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.164 LASEREOL

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Laser Approaching End of Life alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. It is typically accompanied by the “[HI-LASERBIAS](#)” alarm on [page 2-121](#). It is an indicator that the laser in the card must be replaced. How soon the replacement must happen depends upon the HI-LASERBIAS threshold. If the threshold is set under 100 percent, the laser replacement can usually be done during a maintenance window. But if the HI-LASERBIAS threshold is set at 100 percent and is accompanied by data errors, the card must be replaced sooner.

Clear the LASEREOL Alarm

- Step 1** Complete the “[Physically Replace a Traffic Card](#)” procedure on [page 2-271](#).



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on [page 2-260](#) for commonly used traffic-switching procedures.



Note

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.165 LASERTEMP-DEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Laser Temperature Degrade alarm occurs when the Peltier control circuit fails on a DWDM amplifier card such as the OPT-BST or OPT-PRE. The Peltier control provides cooling for the amplifier. The card should be replaced at the next opportunity.

Clear the LASERTEMP-DEG Alarm

- Step 1** For the alarmed DWDM card, complete the “[Physically Replace a Traffic Card](#)” procedure on [page 2-271](#) at the next opportunity.

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.166 LCAS-CRC

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: STSTRM, VT-TERM

The Link Capacity Adjustment Scheme (LCAS) Control Word CRC Failure condition is raised against ML-Series Ethernet cards. It occurs when there is an equipment, path, or provisioning error on the virtual concatenation group (VCG) that causes consecutive 2.5 second CRC failures in the LCAS control word.

Transmission errors would be reflected in CV-P, ES-P, or SES-P performance monitoring statistics. If these errors do not exist, an equipment failure is indicated.

If LCAS is not supported on the peer node, the condition does not clear.

LCAS-CRC can also occur if the VCG source node is not LCAS-enabled, but the receiving node does have the capability enabled. Both source and destination nodes must have LCAS enabled. Otherwise, the LCAS-CRC condition persists on the VCG.



Note

For more information about the ML-Series Ethernet cards, refer to the *<I>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the LCAS-CRC Condition

- Step 1** Look for and clear any associated equipment failures, such as the EQPT alarm, on the receive node or transmit node.
- Step 2** Look for and clear any bit error rate alarms at the transmit node.
- Step 3** If no equipment or SONET path errors exist, ensure that the remote node has LCAS enabled on the circuit:
- In node view, click the **Circuit** tab.
 - Choose the VCAT circuit and click **Edit**.
 - In the Edit Circuit window, click the **General** tab.
 - Verify that the Mode column says **LCAS**.
- Step 4** If the column does not say LCAS, complete the “Delete a Circuit” procedure on page 2-272 and recreate it in LCAS mode using the instructions in the *<I>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.
- Step 5** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.167 LCAS-RX-FAIL

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Receive-Side-In Fail condition is raised against FC_MR-4 cards and ML-Series Ethernet cards with LCAS-enabled VCG.

LCAS VCGs treat failures unidirectionally, meaning that failures of the transmit or receive points occur independently of each other. The LCAS-RX-FAIL condition can occur on the receive side of an LCAS VCG member for the following reasons:

- SONET path failure (a unidirectional failure as seen by the receive side)
- VCAT member is set out of group at the transmit side, but is set in group at the receive side
- VCAT member does not exist at the transmit side but does exist and is in group at the receive side

The condition can be raised during provisioning operations on LCAS VCGs but should clear when the provisioning is completed.

Software-enabled LCAS VCGs treat failure bidirectionally, meaning that both directions of a VCG member are considered failed if either transmit or receive fails. The LCAS-RX-FAIL condition is raised on these VCG members when a member receive side fails due to a SONET path failure.

**Note**

For more information about the ML-Series Ethernet cards, refer to the *<I_Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the LCAS-RX-FAIL Condition

-
- Step 1** Check for and clear any line or path alarms.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.168 LCAS-TX-ADD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Transmit-Side-In Add State condition is raised against ML-Series Ethernet cards when the transmit side of an LCAS VCG member is in the add state. The condition clears after provisioning is completed.

**Note**

LCAS-TX-ADD is an informational condition and does not require troubleshooting.

**Note**

For more information about the ML-Series Ethernet cards, refer to the *<I_Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

2.8.169 LCAS-TX-DNU

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Transmit-Side-In Do Not Use condition is raised on FC_MR-4 cards and ML-Series Ethernet cards when the transmit side of an LCAS VCG member is in the do-not use state. For a unidirectional failure, this condition is only raised at the source node.

The node reporting this condition likely reports an [2.8.295 RFI-P, page 2-213](#), and the remote node likely reports a path alarm such as [2.8.3 AIS-P, page 2-31](#) or [2.8.364 UNEQ-P, page 2-249](#).



Note

LCAS-TX-DNU is an informational condition and does not require troubleshooting.



Note

For more information about the ML-Series Ethernet cards, refer to the *<I_Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

2.8.170 LKOUTPR-S

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Lockout of Protection Span condition occurs when path protection traffic is locked out of a protect span using the Lockout of Protect command.

Clear the LKOUTPR-S Condition

-
- Step 1** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-267.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.171 LOA

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: VCG

The Loss of Alignment on a VCG is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when members of a VCG travel over different paths in the network (due to initial operator provisioning or to protection or restoration events) and the differential delays between the paths cannot be recovered by terminating hardware buffers.



Note

This alarm occurs only if you provision circuits outside of CTC, such as by using TL1.

Clear the LOA Alarm

-
- Step 1** In network view, click the **Circuits** tab.
- Step 2** Click the alarmed VCG and then click **Edit**.
- Step 3** In the Edit Circuit dialog box, click **Show Detailed Map** to see the source and destination circuit slots, ports, and STSs.
- Step 4** Identify whether the STS travels across different fibers. If it does, complete the “[Delete a Circuit](#)” procedure on page 2-272.
- Step 5** Recreate the circuit using the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 6, “Create Circuits and Tunnels.”
- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.172 LOCKOUT-REQ

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN, STSMON, TRUNK, VT-MON

The Lockout Switch Request on Facility or Equipment condition occurs when a user initiates a lockout switch request for an OC-N port in a 1+1 facility protection group. This can be accomplished by locking traffic onto the working port with the LOCK ON command (thus locking it off the protect port), or locking it off the protect port with the LOCK OUT command. In either case, the protect port will show “Lockout of Protection,” and the Conditions window will show the LOCKOUT-REQ condition.

A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ condition.

Clear the LOCKOUT-REQ Condition

-
- Step 1** Complete the “[Clear a Card or Port Lock On or Lock Out Command](#)” procedure on page 2-262.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.173 LOF (BITS)

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: BITS

The Loss of Frame (LOF) BITS alarm occurs when a port on the TCC2/TCC2P BITS input detects an LOF on the incoming BITS timing reference signal. LOF indicates that the receiving ONS 15454 has lost frame delineation in the incoming data.

**Note**

The procedure assumes that the BITS timing reference signal is functioning properly. It also assumes the alarm is not appearing during node turn-up.

Clear the LOF (BITS) Alarm

- Step 1** Verify that the line framing and line coding match between the BITS input and the TCC2/TCC2P:
- In node or card view, note the slot and port reporting the alarm.
 - Find the coding and framing formats of the external BITS timing source. The formats should be in the user documentation for the external BITS timing source or on the timing source itself.
 - Click the **Provisioning > Timing** tabs to display the General Timing window.
 - Verify that Coding matches the coding of the BITS timing source, either B8ZS or AMI.
 - If the coding does not match, click **Coding** and choose the appropriate coding from the drop-down list.
 - Verify that Framing matches the framing of the BITS timing source, either ESF or SF (D4).
 - If the framing does not match, click **Framing** and choose the appropriate framing from the drop-down list.

**Note**

On the timing subtab, the B8ZS coding field is normally paired with ESF in the Framing field and the AMI coding field is normally paired with SF (D4) in the Framing field.

- Step 2** If the alarm does not clear when the line framing and line coding match between the BITS input and the TCC2/TCC2P, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the TCC2/TCC2P.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.174 LOF (DS1)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

The DS-1 LOF alarm indicates that the receiving ONS 15454 has lost frame delineation in an incoming DS-1 data stream. If the LOF appears on the DS1N-14 card, the transmitting equipment could have its framing set to a format that differs from the receiving node.

Clear the LOF (DS1) Alarm

- Step 1** Verify that the line framing and line coding match between the DS1N-14 port and the signal source:
- In CTC, note the slot and port reporting the alarm.
 - Find the coding and framing formats of the signal source for the card reporting the alarm. You might need to contact your network administrator for the format information.
 - Display the card view of the reporting ONS 15454 card.
 - Click the ONS 15454 **Provisioning > Line** tabs.
 - Verify that the line type of the reporting port matches the line type of the signal source (DS4 and DS4, unframed and unframed, or ESF and ESF). If the signal source line type does not match the reporting port, click the **Line Type** cell to reveal a drop-down list and choose the matching type.
 - Verify that the reporting Line Coding matches the signal source line coding (AMI and AMI or B8ZS and B8ZS). If the signal source line coding does not match the reporting port, click the **Line Coding** cell and choose the correct type from the drop-down list.
 - Click **Apply**.



Note On the Line tab, the B8ZS coding field is normally paired with ESF in the Framing field. AMI coding is normally paired with SF (D4) in the Framing field.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.175 LOF (DS3)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: DS3

The DS-3 LOF alarm indicates that the receiving ONS 15454 has lost frame delineation in the incoming DS-3 data stream. The framing of the transmitting equipment could be set to a format that differs from the receiving system. On DS3XM-6 cards, the alarm occurs only on cards with the provisionable framing format set to C Bit or M13 and not on cards with the provisionable framing format is set to unframed.

Clear the LOF (DS3) Alarm

-
- Step 1** Change the line type of the non-ONS equipment attached to the reporting card to C Bit:
- Display the card view of the reporting card.
 - Click the **Provisioning > Line** tabs.
 - Verify that the line type of the reporting port matches the line type of the signal source.
 - If the signal source line type does not match the reporting port, click **Line Type** and choose **C Bit** from the drop-down list.
 - Click **Apply**.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.176 LOF (EC1)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: EC1, EC1-12

The EC1 LOF alarm occurs when a port on the reporting EC1 card has an LOF condition. LOF indicates that the receiving ONS 15454 has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

Clear the LOF (EC1, EC1-12) Alarm

-
- Step 1** Verify cabling continuity to the port reporting the alarm.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.



Note

To verify cable continuity, follow site practices.

- Step 2** If cabling continuity is okay, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”
- Step 3** If the alarm does not clear, see the loopback procedures in [Chapter 1, “General Troubleshooting”](#) to isolate the fault causing the LOF alarm.
- Step 4** If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC to report a service-affecting problem (1 800 553-2447).
-

2.8.177 LOF (OCN)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: OCN

The LOF alarm occurs when a port on the reporting card has an LOF condition. It can also occur on ONS 15454 MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G cards reporting LOF. The alarm indicates that the receiving ONS 15454 has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

When the alarm is raised on an OC-N card, it is sometimes an indication that the OC-N card expects a specific line rate and the input line rate source does not match the input line rate of the optical receiver.

Clear the LOF (OCN) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.



Note

To verify cable continuity, follow site practices.

Step 2 If cabling continuity is okay, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

Step 3 If the alarm does not clear, see the loopback procedures in [Chapter 1, “General Troubleshooting”](#) to isolate the fault causing the LOF alarm.

Step 4 If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.8.178 LOF (TRUNK)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: TRUNK

The Loss of Frame for the DWDM trunk applies to the trunk optical or electrical signal that is carried to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. It indicates that the receiving ONS 15454 has lost frame delineation in the incoming data from trunk that serves the cards. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

Clear the LOF (TRUNK) Alarm

Step 1 Complete the [“Clear the LOF \(OCN\) Alarm”](#) procedure on page 2-143.

- Step 2** If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.8.179 LO-LASERTEMP

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCN

The Equipment Low Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. LO-LASERTEMP occurs when the internally measured transceiver temperature falls below the card setting by 35.6 degrees F or 2 degrees C. A laser temperature change affects the transmitted wavelength. (Two degrees Celsius is equivalent to about 200 picometers in the wavelength.)

When the TXP or MXP card raises this alarm, the laser is automatically shut off. The [“LOS \(OCN\)” alarm on page 2-153](#) is raised at the remote node and the [“DSP-FAIL” alarm on page 2-75](#) is raised at the local node. To verify the card laser temperature level, double-click the card in node view and click the **Performance > Optics PM > Current PM** tabs. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Clear the LO-LASERTEMP Alarm

- Step 1** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for the reporting MXP or TXP card.
- Step 2** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the reporting MXP or TXP card.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.180 LOM

- Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM, TRUNK; Major (MJ) for VT-TERM
- Logical Objects: STSTRM, TRUNK, VT-TERM

The Optical Transport Unit (OTU) Loss of Multiframe is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm applies to MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G cards when the Multi Frame Alignment Signal (MFAS) overhead field is errored for more than five frames and persists for more than 3 milliseconds.

Clear the LOM Alarm

- Step 1** Complete the [“Clear the SD-L Condition” procedure on page 2-220](#).

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.181 LOP-P

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: STSMON, STSTRM

A Loss of Pointer Path alarm indicates that the SONET path pointer in the overhead has been lost. LOP occurs when valid H1/H2 pointer bytes are missing from the overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SONET payload. An LOP-P alarm occurs when eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

The LOP-P alarm can occur when the received payload does not match the provisioned payload. The alarm is caused by a circuit type mismatch on the concatenation facility. For example, if an STS-1 is sent across a circuit provisioned for STS-3c, an LOP-P alarm occurs.

For FC_MR-4 card, an LOP-P is raised if a port is configured for a SONET signal but receives an SONET signal instead. (This information is contained in the H1 byte bits 5 and 6.)

Clear the LOP-P Alarm

- Step 1** In node view, click the **Circuits** tab and view the alarmed circuit.
- Step 2** Verify the circuit size listed in the Size column. If the size is different from what is expected, such as an STS3c instead of an STS1, this causes the alarm.
- Step 3** If you have been monitoring the circuit with optical test equipment, a mismatch between the provisioned circuit size and the size expected by the test set can cause this alarm. Ensure that the test set monitoring is set up for the same size as the circuit provisioning.

For instructions to use the optical test set, consult the manufacturer.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 4** If you have not been using a test set, or if the test set is correctly set up, the error is in the provisioned CTC circuit size. Complete the [“Delete a Circuit” procedure on page 2-272](#).
- Step 5** Recreate the circuit for the correct size. For instructions, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 6, “Create Circuits and Tunnels.”
- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.182 LOP-V

- Default Severity: Major (MJ), Service-Affecting (SA)

- Logical Objects: VT-MON, VT-TERM

The LOP VT alarm indicates a loss of pointer at the VT level.

The LOP-V alarm can occur when the received payload does not match the provisioned payload. LOP-V is caused by a circuit size mismatch on the concatenation facility.

Clear the LOP-V Alarm

-
- Step 1** Complete the “Clear the LOP-P Alarm” procedure on page 2-145.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.183 LO-RXPOWER

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, TRUNK

The Equipment Low Receive Power alarm is an indicator for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G card received optical signal power.

LO-RXPOWER occurs when the measured optical power of the received signal falls under the threshold. The threshold value is user-provisionable.

Clear the LO-RXPOWER Alarm

-
- Step 1** At the transmit end of the errored circuit, increase the transmit power level within safe limits.

- Step 2** Find out whether new channels have been added to the fiber. Up to 32 channels can be transmitted on the same fiber, but the number of channels affects power. If channels have been added, power levels of all channels need to be adjusted.



Note

If the card is part of an amplified DWDM system, adding channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

- Step 3** Find out whether gain (the amplification power) of any amplifiers has been changed. Changing amplification also causes channel power to need adjustment.

- Step 4** If the alarm does not clear, remove any receive fiber attenuators or replace them with lower-resistance attenuators.

- Step 5** If the alarm does not clear, inspect and clean the receive and transmit node fiber connections according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

Step 6 If the alarm does not clear, ensure that the fiber is not broken or damaged by testing it with an optical test set. If no test set is available, use the fiber for a facility (line) loopback on a known-good port. The error readings you get is not as precise, but you generally know whether the fiber is faulty.

For specific procedures to use the test set equipment, consult the manufacturer.

Step 7 If the alarm does not clear, and no faults are present on the other port(s) of the transmit or receive card, do a facility loopback on the transmit and receive ports with known-good loopback cable. Complete the “[1.4.1 Perform a Facility \(Line\) Loopback on a Source-Node Optical Port](#)” procedure on page 1-47 or the “[1.4.4 Perform a Facility \(Line\) Loopback on an Intermediate-Node Optical Port](#)” procedure on page 1-56 to test the loopback.

Step 8 If a port is bad and you need to use all the port bandwidth, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 9 If no ports are shown bad and the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.184 LOS (2R)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: 2R

The Loss of Signal for a 2R Client applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. The alarm is raised when the card port is not receiving input. An AIS is sent upstream.

Clear the LOS (2R) Alarm

Step 1 Complete the “[Clear the LOS \(OCN\) Alarm](#)” procedure on page 2-153.

Step 2 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.185 LOS (BITS)

- Default Severity: Minor (MN), Non-Service Affecting (NSA)

- Logical Object: BITS

The LOS (BITS) alarm indicates that the TCC2/TCC2P has an LOS from the BITS timing source. The LOS (BITS) means the BITS clock or the connection to the BITS clock failed.

Clear the LOS (BITS) Alarm

-
- Step 1** Verify the wiring connection from the BITS clock pin fields on the ONS 15454 backplane to the timing source.



Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 2** If wiring is good, verify that the BITS clock is operating properly.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.186 LOS (DS1)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

A LOS (DS1) alarm for a DS-1 port occurs when the port on the card is in service but no signal is being received. The cabling is not correctly connected to the card, or no signal exists on the line.

Clear the LOS (DS1) Alarm

-
- Step 1** Verify that the fiber cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”



Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 2** Consult site records to determine whether the port raising the alarm has been assigned.
- Step 3** If the port is not currently assigned, place the port out of service using the following steps:
- Double-click the card to display the card view.
 - For a DS1 card, click the **Maintenance > Loopback** tabs. For a DS-1 line on a DS3XM-6 or DS3XM-12 card, click the **Maintenance > DS1** tabs.
 - Under Admin State, click **OOS,DSBLD**.
 - Click **Apply**.
- Step 4** If the port is assigned, verify that the correct port is in service:
- To confirm this physically, confirm that the LED is correctly illuminated on the physical card.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

- b. To determine this virtually, double-click the card in CTC to display the card view:
 - Click the **Provisioning > Line** tabs.
 - Verify that the Admin State column lists the port as IS.
 - If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

- Step 5** Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible. For specific procedures to use the test set equipment, consult the manufacturer.
- Step 6** Ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected. For more information about fiber connections and terminations, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”
- Step 7** If there is a valid signal, replace the electrical connector on the ONS 15454.
- Step 8** If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port. To do this, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”
- Step 9** Repeat Steps 1 to 8 for any other port on the card that reports the LOS.
- Step 10** If no other alarms are present that could be the source of the LOS (DS-1), or if clearing an alarm did not clear the LOS, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the reporting card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 11** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.187 LOS (DS3)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: DS3

The LOS (DS3) for a DS-3 port occurs when the port on the card is in service but no signal is being received. The cabling is not correctly connected to the card, or no signal exists on the line. Possible causes for no signal on the line include upstream equipment failure or a fiber cut.

**Note**

If a circuit shows a partial status when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (DS3) Alarm

Step 1 Complete the “[Clear the LOS \(DS1\) Alarm](#)” procedure on page 2-148.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.188 LOS (EC1, EC1-12)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: EC1, EC1-12

LOS on an EC1/EC1-12 port occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS (EC1/EC1-12) means that the upstream transmitter has failed. If an EC1-12 LOS alarm is not accompanied by additional alarms, a cabling problem is usually the cause of the alarm. The condition clears when two consecutive valid frames are received.



Note

If a circuit shows a partial status when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (EC1, EC1-12) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.



Note To verify cable continuity, follow site practices.

Step 2 If the cabling is okay, verify that the correct port is in service:

- Confirm that the LED is correctly lit on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- To determine whether the port is in service, double-click the card in CTC to display the card view.
- Click the **Provisioning > Line** tabs.
- Verify that the Admin State column lists the port as IS.
- If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

- Step 3** If the correct port is in service, use an optical test set to confirm that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.
- Step 4** If the signal is valid, ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected. For more information about fiber connections and terminations, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”
- Step 5** If a valid signal exists, replace the cable connector on the ONS 15454.
- Step 6** Repeat Steps 1 through 5 for any other port on the card that reports the LOS (EC1).
- Step 7** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.
- Step 8** If no other alarms exist that could be the source of the LOS (EC1), or if clearing an alarm did not clear the LOS, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the reporting card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 9** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.189 LOS (ESCON)

The LOS alarm for ESCON is not used in this platform in this release. It is reserved for future development.

2.8.190 LOS (FUDC)

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: FUDC

The LOS (FUDC) alarm is raised if there is a UDC circuit created on an AIC-I UDC port but the port is not receiving signal input. The downstream node has an AIS condition raised against the AIC-I port transmitting the UDC. FUDC refers to the 64-kb user data channel using the F1 byte.

Clear the LOS (FUDC) Alarm

- Step 1** Verify cable continuity to the AIC-I UDC port.



Note To verify cable continuity, follow site practices.

- Step 2** Verify that there is a valid input signal using a test set.
- Step 3** If there is a valid signal, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”
- Step 4** If the alarm does not clear, verify that the UDC is provisioned:
- a. At the network view, click the **Provisioning > Overhead Circuits** tabs.
 - b. If no UDC circuit exists, create one. Refer to the *Cisco ONS 15454 Procedure Guide* Chapter 6, “Create Circuits and VT Tunnels.”
 - c. If a user data circuit exists (shown as User Data F1 under the Type column), check the source and destination ports. These must be located on AIC-I cards to function.
- Step 5** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.
- Step 6** If no other alarms exist that could be the source of the LOS (FUDC), or if clearing another alarm did not clear the LOS, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the reporting card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 7** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.191 LOS (ISC)

- Default Severity: Critical (CR), Service Affecting (SA)
- Logical Object: ISC

The LOS alarm for the ISC port applies to TXP_MR_2.5G client PPMs provisioned at the ISC port rate. Troubleshooting is similar to the LOS (2R) alarm.

Clear the LOS (ISC) Alarm

-
- Step 1** Complete the “[Clear the LOS \(2R\) Alarm](#)” procedure on page 2-147.

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.192 LOS (MSUDC)

The LOS (MSUDC) alarm is not used in this platform in this release. It is reserved for future development.

2.8.193 LOS (OCN)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: OCN

An LOS alarm on an OC-N port occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS alarm means the upstream transmitter has failed. If an OC-N LOS alarm is not accompanied by additional alarms, a fiber break is usually the cause of the alarm. The condition clears when two consecutive valid frames are received.



Warning

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057



Note

If a circuit shows a partial status when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (OCN) Alarm

- Step 1** Verify fiber continuity to the port.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.



Note To verify fiber continuity, follow site practices.

- Step 2** If the cabling is okay, verify that the correct port is in service:
- a. Confirm that the LED is correctly illuminated on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 - b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
 - c. Click the **Provisioning > Line** tabs.
 - d. Verify that the Admin State column lists the port as IS.
 - e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**.
 - f. Click **Apply**.
- Step 3** If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”
- Step 4** If the alarm does not clear, verify that the power level of the optical signal is within the OC-N card receiver specifications. The “[1.13.3 OC-N Card Transmit and Receive Levels](#)” section on page 1-154 lists these specifications for each OC-N card. For DWDM cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for levels.
- Step 5** If the optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line.
For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.
- Step 6** If a valid signal exists, replace the connector on the backplane.
- Step 7** Repeat Steps 1 to 6 for any other port on the card reporting the LOS (OC-N).
- Step 8** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.
- Step 9** If no other alarms exist that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the reporting card.



Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 10** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.194 LOS (OTS)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: OTS

The Loss of Signal for the OTS applies to the LINE-3-RX port of the OPT-BST amplifier and the LINE-2-RX port of the OSCM or OSC-CSM card. It indicates that a fiber cut has occurred and no power is being received from the span. The alarm is raised when both LOS-P and LOS-O alarms occur, and demotes them.

Clear the LOS (OTS) Alarm

Step 1 Verify fiber continuity to the port.



Note To verify fiber continuity, follow site practices.

Step 2 If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 3 Verify that the received power (opwrMin value of the Line 4-1-RX port) is within the expected range shown in Cisco MetroPlanner. To check the level:

- Double-click the amplifier card to display the card view.
- Click the **Provisioning > Opt. Ampli. Line > Optics Thresholds** tabs.
- Compare the opwrMin (dBm) column value with the MetroPlanner-generated value. (For more information about using MetroPlanner, refer to the *Cisco MetroPlanner DWDM Operations Guide*.)

Step 4 If the optical power level is within specifications, check and modify the channel LOS and OSC LOS thresholds, then run automatic node setup (ANS) to execute the changes. (For more information about ANS, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

- In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.
- Consult the *Cisco MetroPlanner DWDM Operations Guide* to decide what values to use, then modify the following items:
 - West Side Rx. Channel OSC LOS Threshold
 - West Side Rx. Channel LOS Threshold
- Click the **WDM-ANS > Port Status** tabs.
- Click **Launch ANS** and click **Yes** in the confirmation dialog box.

Step 5 If the optical power is outside of the expected range, check the power level transmitted at the other side of the span using CTC:

- On the transmitting node, double-click the transmitting MXP or TXP to display the card view.
- Click the **Provisioning > Optics Thresholds** tab.
- View the TX Power High and TX Power Low values, comparing them with the MetroPlanner-generated values.

Step 6 If the transmitted power value is within the expected range, clean the receiving node (where the LOS is raised) and clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

- Step 7** If the transmitted power value is outside of the expected range, troubleshoot using the DWDM acceptance tests in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.
- Step 8** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.
- Step 9** If no other alarms exist that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the reporting card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 10** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.195 LOS (TRUNK)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: TRUNK

The Loss of Signal for a TRUNK applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. The alarm is raised when the card port is not receiving input. An AIS is sent upstream.

Clear the LOS (TRUNK) Alarm

- Step 1** Verify fiber continuity to the port.

**Note**

To verify fiber continuity, follow site practices.

- Step 2** If the cabling is okay, verify that the correct port is in service:
- Confirm that the LED is correctly illuminated on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 - To determine whether the port is in service, double-click the card in CTC to display the card view.
 - Click the **Provisioning > Line** tabs.
 - Verify that the Admin State column lists the port as IS.
 - If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

- Step 3** If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”
- Step 4** If the alarm does not clear, verify that the power level of the optical signal is within the TXP or MXP card receiver specifications. Refer to the *<I_Ital>Cisco ONS 15454 Reference Manual* for levels.
- Step 5** If the optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line.
For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.
- Step 6** If a valid signal exists, replace the connector on the backplane.
- Step 7** Repeat Steps 1 to 6 for any other port on the card reporting the LOS (TRUNK).
- Step 8** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.
- Step 9** If no other alarms exist that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the reporting card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 10** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.196 LOS-0

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: OCH, OMS, OTS

The Incoming Overhead Loss of Signal alarm applies to the OSC-RX port of OPT-BST (LINE-2-RX), the OSC-RX port of OSCM (LINE-1-RX), and the internal optical port of OSC-CSM card (LINE-3-RX Port 3). It is raised when the monitored input power crosses the FAIL-LOW threshold and the OSC signal is lost. The alarm is demoted if another LOS alarm is also present.

Clear the LOS-0 Alarm

- Step 1** Verify fiber continuity to the port.

**Note**

To verify fiber continuity, follow site practices.

- Step 2** If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.
- Step 3** Verify that the received power (opwrMin) is within the expected range shown in Cisco MetroPlanner. To check the level:
- Double-click the amplifier card to display the card view.
 - Display the optical thresholds by clicking the following tabs:
 - OPT-BST Provisioning > Opt. Ampli. Line > Optics Thresholds tab
 - OSCM or OSC-CSM Provisioning > Optical Line > Optics Thresholds tab
- Step 4** If the optical power level is within specifications, check and modify the OSC LOS threshold, then run ANS to execute the changes. (For more information about ANS, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)
- In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.
 - Consult the *Cisco MetroPlanner DWDM Operations Guide* to decide upon values, then modify the West Side Rx. Channel OSC LOS Threshold.
 - Click the **WDM-ANS > Port Status** tabs.
 - Click **Launch ANS** and click **Yes** in the confirmation dialog box.
- Step 5** If the port power is outside of the expected range, verify that OSC connections have been created on the other side of the span. If the connections are not present, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for procedures.
- Step 6** If OSC connections are present, check the OSC transmitted power using CTC:
- On the transmitting node, double-click the transmitting OSC-CSM to display the card view.
 - Click the **Provisioning > Optics Thresholds** tab.
 - View the TX Power High and TX Power Low values, comparing them with the MetroPlanner-generated values.
- Step 7** If the transmitted OSC value is out of range, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for DWDM acceptance test procedures that aids in troubleshooting the problem.
- Step 8** If the OSC value is within range, come back to the port reporting the LOS-O alarm and clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”
- Step 9** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.
- Step 10** If no other alarms exist that could be the source of the LOS-O, or if clearing an alarm did not clear the LOS-O, place all of the card ports in OOS,DSBLD admin state.
- Step 11** Complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the reporting card.



Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external traffic switch if possible.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database apart from restoring the card's port to the IS,AINS admin state.

- Step 12** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.197 LOS-P (OCH)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OCH

The Loss of Signal for Optical Channel alarm on the OCH layer applies to the channel ADD or pass-through ports on the AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, 32MUX-O and 32WSS-O DWDM cards.



Note

For 32WSS-O cards, this alarm also applies to pass-through ports. If the LOS-P (OCH) alarm is raised against this kind of port, it means that the port does not have an optical power source directly connected to it. Follow the general troubleshooting rules stated in the chapter Network Level (inter-nodes) Troubleshooting to identify upstream alarms in the logical signal flow that could cause an LOS-P.

LOS-P (OCH) indicates a loss of receive signal when the monitored input power value has crossed the Power Failure Low threshold associated with the port. This threshold value is relative to the specific variable optical attenuation (VOA) power reference setpoint provisioned on VOA along the path.

Clear the LOS-P (OCH) Alarm

- Step 1** Check the LED behavior on the physical card. A green ACT/SBY LED indicates an active card, and a red ACT/SBY LED indicates a failed card. If the LED is red, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) and continue to [Step 9](#).
- Step 2** Verify that there truly is a loss of received signal:
- Double-click the card to open the card view.
 - View the proper input power values by clicking one of the following tabs as appropriate:
 - For the AD-xC card, click the **Provisioning > Optical Chn > Parameters** tabs.
 - For the 32MUX-O card, click the **Provisioning > Optical Chn > Parameters** tabs.
 - For the 32WSS-O card, click the **Provisioning > Optical Chn: Optical Connector x > Parameters** tabs.
 - Display the proper Power Failure Low threshold by clicking one of the following tabs as appropriate:
 - For the AD-xC card, click the **Provisioning > Optical Chn > Optics Thresholds** tabs.
 - For the 32MUX-O card, click the **Provisioning > Optical Chn > Optics Thresholds** tabs.
 - For the 32WSS-O card, click the **Provisioning > Optical Chn: Optical Connector x > Optics Thresholds** tabs.



Tip

To view the alarm thresholds (as opposed to the warning thresholds), check the **Alarm** check box on the Optics Thresholds tab and click **Reset**.

- d. Compare the actual assigned Power value with the Alarm Threshold value and complete one of the following actions:
- If the Power value is less than the Fail Low threshold, go to [Step 3](#).
 - If the Power value is greater than the Fail Low threshold plus the alarm allowance value (default 1 dBm), complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for the card.

If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) and continue to [Step 9](#).

- Step 3** Verify the fiber continuity to the port. To verify fiber continuity, follow site practices.
- Step 4** In MetroPlanner, obtain the “Internal Connections” file for the node where the errored card is located. If necessary, correct the node cabling in accordance with the MP file connections list. For procedures to cable a DWDM node, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.
- Step 5** If the cabling is good, verify that each involved optical signal source, including TXP, MXP or ITU-T line card trunk transmit ports, is in the IS admin state. To do this, click the following tabs as appropriate:
- For the TXP_MR_10G card, click the **Provisioning > Line > SONET** tabs.
 - For the TXP_MR_10E card, click the **Provisioning > Line > SONET** tabs.
 - For the TXP_MR_2.5G card, click the **Provisioning > Line > SONET** tabs.
 - For the TXPP_MR_2.5G card, click the **Provisioning > Line > OC48** tabs.
 - For the MXP_MR_2.5G card, click the **Provisioning > Line > OC48** tabs.
 - For the MXPP_MR_2.5G card, click the **Provisioning > Line > OC48** tabs.
 - For the MXP_2.5G_10E card, click the **Provisioning > Line > Trunk** tabs.
 - For the MXP_2.5G_10G card, click the **Provisioning > Line > SONET** tabs.
- If the port admin state is not IS, choose IS from the **Admin state** drop-down list. If the alarm does not clear, continue with [Step 6](#).
- Step 6** If the signal source is in IS admin state, use an optical test set to verify that the transmit laser is active. For specific procedures to use the test set equipment, consult the manufacturer.
- Step 7** If the laser is active, compare the card’s provisioned transmit optical power value with the expected range in the “Hardware Specifications” appendix of the *Cisco ONS 15454 Procedure Guide*. To display the provisioned transmit optical power values, click the following tabs as appropriate:
- For the TXP_MR_10G card, click the **Performance > Optics PM > Current Values > Trunk Port** tabs.
 - For the TXP_MR_10E card, click the **Performance > Optics PM > Current Values > Trunk Port** tabs.
 - For the MXP_2.5G_10E card, click the **Performance > Optics PM > Current Values > Trunk Port** tabs.
 - For the MXP_2.5G_10G card, click the **Performance > Optics PM > Current Values > Trunk Port** tabs.
- Step 8** Use an optical test set to measure actual transmit optical power for the following cards as applicable:
- TXP_MR_2.5G
 - TXPP_MR_2.5G
 - MXP_MR_2.5G
 - MXPP_MR_2.5G
 - Each ITU-T line card

If the tested optical transmit optical power is comparable to the correctly provisioned value and the expected value, go to [Step 9](#). If the tested, actual power value is outside the specification range, complete the “[Physically Replace a Traffic Card](#)” procedure on [page 2-271](#). When the newly installed card becomes active, verify that the LOS-P (OCH) alarm clears. If it does not, continue with [Step 9](#).

**Tip**

If a spare cards is unavailable and the transmit power still functions, you can temporarily clear the LOS-P alarm by following the general procedure to add path VOAs during startup failure located in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 9

If the power is within the expected range, clean the alarmed port’s fiber according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter of the *Cisco ONS 15454 Procedure Guide*.

**Note**

Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on [page 2-260](#) for basic instructions, or refer to the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide* for more detailed information.

Step 10

If the alarm does not clear, follow the general procedure for adding path VOAs during startup failure in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Step 11

If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.198 LOS-P (OMS, OTS)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: OMS, OTS

The Loss of Signal for Optical Channel alarm (OMS or OTS layer) applies to all input ports of the following DWDM cards: AD-1B-xx.x, AD-4B-xx.x, 32 DMX, 32DMX-O, OPT-PRE, OPT-BST, and OSC-CSM.

For AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, 32MUX-O and 32WSS cards, this alarm applies only to the COM-RX, EXP-RX, xxBAND-RX input ports where an aggregate signal is managed. (These ports are solely used for the OMS and OTS layers.)

LOS-P (OMS or OTS) indicates a loss of receive signal when the monitored input power value has crossed the Power Failure Low Threshold associated to the port.

**Note**

When the LOS-P alarm is raised on the LINE-RX port of the OPT-BST or OSC-CSM card, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for a fiber cut detection procedure.

Clear the LOS-P (OMS, OTS) Alarm

- Step 1** Check the LED behavior on the physical card. A green ACT/SBY LED indicates an active card, and a red ACT/SBY LED indicates a failed card. If the LED is red, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) and continue to [Step 7](#).
- Step 2** Verify that there truly is a loss of input signal:
- a. Double-click the card to open the card view.
 - b. Verify the proper input power values by clicking one of the following tabs as appropriate:
 - For the OPT-BST card, click the **Provisioning > Optical Line > Parameters** tabs.
 - For the OPT-PRE card, click the **Provisioning > Optical Line > Parameters** tabs.
 - For the AD-xC card, click the **Provisioning > Optical Line > Parameters** tabs.
 - For the AD-xB card, click the **Provisioning > Optical Line > Parameters** tabs.
 - For the AD-xB card, click the **Provisioning > Optical Line > Parameters** tabs.
 - For the 32MUX-O card, click the **Provisioning > Optical Line > Parameters** tabs.
 - For the 32WSS card, click the **Provisioning > Optical Line > Parameters** tabs.
 - For the 32DMX-O card, click the **Provisioning > Optical Line > Parameters** tabs.
 - For the 32DMX card, click the **Provisioning > Optical Line > Parameters** tabs.
 - For the OSC-CSM card, click the **Provisioning > Optical Line > Parameters** tabs.
 - c. Display the proper Power Failure Low threshold by clicking one of the following tabs as appropriate:
 - For the OPT-BST card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
 - For the OPT-PRE card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
 - For the AD-xC card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
 - For the AD-xB card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
 - For the AD-xB card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
 - For the 32MUX-O card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
 - For the 32WSS card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
 - For the 32DMX-O card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
 - For the 32DMX card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
 - For the OSC-CSM card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.



Tip

To view the alarm thresholds (as opposed to the warning thresholds), check the **Alarm** check box on the Optics Thresholds tab and click **Reset**.

- d. Compare the actual assigned Power value with the Alarm Threshold value and complete one of the following actions:
 - If the Power value is less than the Fail Low threshold, go to [Step 3](#).
 - If the Power value is greater than the Fail Low threshold plus the alarm allowance value (default 1 dBm), complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for the card.

If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) and continue to [Step 7](#).

- Step 3** Verify the fiber continuity to the port. To verify fiber continuity, follow site practices.
- Step 4** In MetroPlanner, obtain the “Internal Connections” file for the node where the errored card is located. If necessary, correct the node cabling in accordance with the MP file connections list. To cable a DWDM node, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.
- Step 5** If the cabling is good, use an optical test set to measure the power value on the output port connected to the alarmed card. For specific procedures to use the test set equipment, consult the manufacturer. If the power difference reported is greater than 1 dBm (standard fiber jumper insertion loss is 0.3 dBm), clean the fiber according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter of the *Cisco ONS 15454 Procedure Guide*.



Note Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for basic instructions, or to the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide* for more detailed information.

- Step 6** If the alarm does not clear, follow the general troubleshooting for identifying upstream alarms in the logical signal flow (that could cause an LOS-P) located in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.
- Step 7** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.199 LOS-P (TRUNK)

Default Severity: Critical (CR), Service-Affecting (SA)


Logical Object: TRUNK

The Loss of Signal for Optical Channel alarm indicates that no optical power is detected at the input trunk port for the following cards:

- TXP_MR_10G
- TXP_MR_10E
- MXP_2.5G_10E
- MXP_2.5G_10G
- TXP_MR_2.5G
- TXPP_MR_2.5G
- MXP_MR_2.5G
- MXPP_MR_2.5G
- All ITU-T line cards

Clear the LOS-P (TRUNK) Alarm

-
- Step 1** Check the LED behavior on the physical card. A green ACT/SBY LED indicates an active card, and a red ACT/SBY LED indicates a failed card. If the LED is red, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 and continue to [Step 7](#).

- Step 2** Verify that there truly is a loss of received optical power:
- Double-click the alarmed card to open the card view.
 - Click the **Performance > Optics PM > Current Values > Trunk Port** tab.
 - Compare the actual received power levels with the expected power range given in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Then take one of the following actions:
 - If power is less than -40 dBm, go to [Step 6](#).
 - If power is greater than -40 dBm and within the expected range, complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-268 for the card.
- Step 3** If the alarm does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the reporting card and then go to [Step 9](#).
- Step 4** Verify the fiber continuity to the port. To verify fiber continuity, follow site practices.
- Step 5** In MetroPlanner, obtain the “Internal Connections” file for the node containing the alarmed card. If necessary, correct the node cabling in accordance with the MP file connections list. For procedures to cable a DWDM node, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.
- Step 6** If the cabling is good, use a test set to verify the power value on the DWDM CH_DROP-TX port on the AD-xC, 32DMX-O, or 32DMX. For specific procedures to use the test set equipment, consult the manufacturer.
- Step 7** If the power difference reported is greater than 1 dBm (standard fiber jumper insertion loss is 0.3 dBm), clean the fiber according to site practice. If no site practice exists, complete the procedure in the “Maintain the Node” chapter of the *Cisco ONS 15454 Procedure Guide*.
-
-  **Note** Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for basic instructions, or to the “Maintain the Node” chapter in the *Cisco ONS 15454 Procedure Guide* for more detailed information.
-
- Step 8** If the alarm does not clear, follow the general troubleshooting rules stated in the chapter Network Level (inter-nodes) Troubleshooting to identify upstream alarms in the logical signal flow that could cause an LOS-P.
- Step 9** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.200 LO-TXPOWER

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, PPM, TRUNK

The Equipment Low Transmit Power alarm is an indicator for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G card transmitted optical signal power. LO-TXPOWER occurs when the measured optical power of the transmitted signal falls under the threshold. The threshold value is user-provisionable.

Clear the LO-TXPOWER Alarm

-
- Step 1** Display the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G card view.
- Step 2** Click the **Provisioning > Optical Thresholds** tabs.
- Step 3** Increase the TX Power Low column value by 0.5 dBm.
- Step 4** If the card transmit power setting cannot be increased without affecting the signal, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 5** If no ports are shown bad and the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.201 LPBKCRS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: STSMON

The Loopback Cross-Connect condition indicates that there is a software cross-connect loopback active between an optical card and an XC10G card. A cross-connect loopback test occurs below line speed and does not affect traffic.

For more information on loopbacks, see the “[1.4 Troubleshooting Optical Circuit Paths With Loopbacks](#)” section on page 1-47.

**Note**

Cross-connect loopbacks occur below line speed. They do not affect traffic.

Clear the LPBKCRS Condition

-
- Step 1** To remove the loopback cross-connect condition, double-click the optical card in CTC to display the card view.
- Step 2** Complete the “[Clear an OC-N Card Cross-Connect \(XC\) Loopback Circuit](#)” procedure on page 2-273.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.202 LPBKDS1FEAC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A Loopback Caused by Far-End Alarm and Control (FEAC) Command DS-1 condition on DS3XM-6 and DS3XM-12 cards occurs when a DS-1 loopback signal is received from the remote-node node due to a FEAC command. An FEAC command is often used with loopbacks.



Caution

CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKDS1FEAC Condition

-
- Step 1** In node view, double-click the DS3XM-6 or DS3XM-12 card to display the card view.
- Step 2** Click the **Maintenance > DS1** tabs.
- Step 3** Click the cell for the port in the Send Code column and click **No Code** from the drop-down list.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.203 LPBKDS1FEAC-CMD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS1

The DS-1 Loopback Command Sent To Far End condition occurs on the local node when you send a DS-1 FEAC loopback. For more information about FEAC loopbacks, see the [“1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks”](#) section on page 1-45.



Note

LPBKDS1FEAC-CMD is an informational condition and does not require troubleshooting.



Caution

CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

2.8.204 LPBKDS3FEAC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

A Loopback Due to FEAC Command DS-3 condition occurs when a DS3XM-6, DS3XM-12, DS3-12E, or DS3/EC1-48 card loopback signal is received in C-bit framing mode from the remote-node node because of an FEAC command. An FEAC command is often used with loopbacks. LPBKDS3FEAC is only reported by these DS cards. DS3XM-6, DS3XM-12, and DS3/EC1-48 cards generate and report FEAC alarms or conditions, but a DS3-12E card only reports FEAC alarms or conditions.

**Caution**

CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are service-affecting.

**Note**

LPBKDS3FEAC is an informational condition and does not require troubleshooting.

Clear the LPBKDS3FEAC Condition

-
- Step 1** In node view, double-click the DS-3 card to display the card view.
- Step 2** Click the **Maintenance > DS3** tabs.
- Step 3** Click the cell for the port in the Send Code column and click **No Code** from the drop-down list.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.205 LPBKDS3FEAC-CMD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS3

The DS-3 Loopback Command Sent To Far End condition occurs on the local node when you send a DS-3 FEAC loopback. For more information about FEAC loopbacks, see the [“1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks”](#) section on page 1-45.

**Note**

LPBKDS3FEAC-CMD is an informational condition and does not require troubleshooting.

2.8.206 LPBKFACILITY (CE100T)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: CE100T

A Loopback Facility condition on a CE-100T-8 port occurs when a software facility (line) loopback is active for a port on the card.

For information about troubleshooting Ethernet circuits, refer to the [“1.5 Troubleshooting Ethernet Circuit Paths With Loopbacks”](#) section on page 1-69.

Clear the LPBKFACILITY (CE100T) Condition

-
- Step 1** Complete the [“Clear an Ethernet Card Loopback Circuit”](#) procedure on page 2-275.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.207 LPBKFACILITY (DS1, DS3)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A Loopback Facility condition occurs when a software facility (line) loopback is active for a DS1 or DS3 port on the reporting DS3XM-6 or DS3XM-12 card.

For information about troubleshooting electrical circuits, refer to the “[1.2 Troubleshooting Electrical Circuit Paths With Loopbacks](#)” section on page 1-9.


Note

CTC permits loopbacks to be performed on an in-service (IS) circuit. Performing a loopback is service-affecting. If you did not perform a lockout or Force switch to protect traffic, the LPBKFACILITY condition can be accompanied by a more serious alarms such as LOS.


Note

DS-3 facility (line) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted to the loopback is provided.

Clear the LPBKFACILITY (DS1, DS3) Condition

- Step 1** Complete the “[Clear a DS3XM-6 or DS3XM-12 Card Loopback Circuit](#)” procedure on page 2-273.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.208 LPBKFACILITY (EC1)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EC1

A Loopback Facility condition occurs when a software facility (line) loopback is active for a port on the reporting EC1 card.

For information about troubleshooting electrical circuits, refer to the “[1.2 Troubleshooting Electrical Circuit Paths With Loopbacks](#)” section on page 1-9.


Caution

CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (EC1, EC1-12) Condition

- Step 1** Complete the “[Clear Other DS-N Card, EC-1, or G1000 Card Loopbacks](#)” procedure on page 2-274.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.209 LPBKFACILITY (ESCON)

The LPBKFACILITY condition for ESCON is not used in this platform in this release. It is reserved for future development.

2.8.210 LPBKFACILITY (FC)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FC

A Loopback Facility condition occurs on a fibre channel (FC) line when a software facility (line) loopback is active for an MXPP_MR_2.5G or TXPP_MR_2.5G card client PPM provisioned at the FC1G or FC2G line speed.

For information about troubleshooting these circuits, refer to the “[1.6 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks](#)” section on page 1-87.

Clear the LPBKFACILITY (FC) Condition

-
- Step 1** Complete the “[Clear an MXP, TXP, or FC_MR Card Loopback Circuit](#)” procedure on page 2-274.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.211 LPBKFACILITY (FCMR)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FCMR

A Loopback Facility for FC_MR condition occurs when a facility loopback is provisioned on an FC_MR-4 card.

For information about troubleshooting these circuits, refer to the “[1.6 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks](#)” section on page 1-87.

Clear the LPBKFACILITY (FCMR) Condition

-
- Step 1** Complete the “[Clear an MXP, TXP, or FC_MR Card Loopback Circuit](#)” procedure on page 2-274.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.212 LPBKFACILITY (G1000)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: G1000

A Loopback Facility condition for the G1000 object occurs when a software facility (line) loopback is active for a port on the reporting G-Series Ethernet card.

For information about troubleshooting Ethernet circuits, refer to the “[1.5 Troubleshooting Ethernet Circuit Paths With Loopbacks](#)” section on page 1-69.



Caution

CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (G1000) Condition

-
- Step 1** Complete the “[Clear Other DS-N Card, EC-1, or G1000 Card Loopbacks](#)” procedure on page 2-274.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.213 LPBKFACILITY (GE)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: GE

A Loopback Facility condition for a Gigabit Ethernet (GE) port occurs when a software facility (line) loopback is active for an MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, or TXPP_MR_2.5G card client PPM provisioned at the ONE_GE port rate. For the TXP_MR_10E and TXP_MR_10G cards, this condition occurs when there is a facility loopback on a client PPM provisioned at the TEN_GE port rate.

For information about troubleshooting these circuits, refer to the “[1.6 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks](#)” section on page 1-87.

Clear the LPBKFACILITY (GE) Condition

-
- Step 1** Complete the “[Clear an MXP, TXP, or FC_MR Card Loopback Circuit](#)” procedure on page 2-274.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.214 LPBKFACILITY (ISC)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: ISC

A Loopback Facility condition for an ISC port occurs when a software facility (line) loopback is active for a TXP_MR_2.5G client PPM provisioned at the ISC port rate.

For information about troubleshooting these circuits, refer to the “[1.6 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks](#)” section on page 1-87.

Clear the LPBKFACILITY (ISC) Condition

-
- Step 1** Complete the “[Clear an MXP, TXP, or FC_MR Card Loopback Circuit](#)” procedure on page 2-274.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.215 LPBKFACILITY (OCN)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

A Loopback Facility condition occurs when a software facility (line) loopback is active for a port on the reporting OC-N card.

For information about troubleshooting optical circuits, refer to the “[1.4 Troubleshooting Optical Circuit Paths With Loopbacks](#)” section on page 1-47.

**Note**

OC-3 facility loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted to the loopback is provided.

**Caution**

CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (OCN) Condition

-
- Step 1** Complete the “[Clear an OC-N Card Facility or Terminal Loopback Circuit](#)” procedure on page 2-273.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

**Caution**

Before performing a facility (line) loopback on an OC-N card, ensure that the card contains at least two DCC paths to the node where the card is installed. A second DCC path provides a nonlooped path to log into the node after the loopback is applied, thus enabling you to remove the facility loopback. Ensuring a second DCC is not necessary if you are directly connected to the ONS 15454 containing the loopback OC-N.

2.8.216 LPBKFACILITY (TRUNK)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

A Loopback Facility condition on MXP and TXP card client port indicates that there is an active facility (line) loopback on the port. For this condition to be present, the admin state is OOS,MT and the service state is OOS-MA, LPBK & MT.

For information about troubleshooting these circuits, refer to the “[1.6 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks](#)” section on page 1-87.

**Caution**

CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (TRUNK) Condition

-
- Step 1** Complete the “[Clear an MXP, TXP, or FC_MR Card Loopback Circuit](#)” procedure on page 2-274.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.217 LPKTERMINAL (CE100T)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: CE100T

A Loopback Terminal condition on a CE-100T-8 port occurs when a software terminal loopback is active for a port on the card.

For information about troubleshooting Ethernet circuits, refer to the “[1.5 Troubleshooting Ethernet Circuit Paths With Loopbacks](#)” section on page 1-69.

Clear the LPBKTERMINAL (CE100T) Condition

-
- Step 1** Complete the “[Clear an Ethernet Card Loopback Circuit](#)” procedure on page 2-275.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.218 LPBKTERMINAL (DS1, DS3)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A Loopback Terminal condition occurs when a software terminal (inward) loopback is active for a DS1 or DS3 port on the reporting DS3XM-6 or DS3XM-12 card. DS-1 and DS-3 terminal loopbacks do not typically return an AIS signal.

For information about troubleshooting electrical circuits, refer to the “[1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks](#)” section on page 1-45.

Clear the LPBKTERMINAL (DS1, DS3) Condition

-
- Step 1** Complete the “[Clear a DS3XM-6 or DS3XM-12 Card Loopback Circuit](#)” procedure on page 2-273.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.219 LPBKTERMINAL (EC1)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EC1

A Loopback Terminal condition occurs when a software terminal (inward) loopback is active for a port on the reporting EC1 card.

For information about troubleshooting electrical circuits, refer to the “[1.2 Troubleshooting Electrical Circuit Paths With Loopbacks](#)” section on page 1-9.

**Caution**

CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKTERMINAL (EC1, EC1-12) Condition

-
- Step 1** Complete the “[Clear Other DS-N Card, EC-1, or G1000 Card Loopbacks](#)” procedure on page 2-274.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.220 LPBKTERMINAL (ESCON)

The LPBKTERMINAL condition for ESCON is not used in this platform in this release. It is reserved for future development.

2.8.221 LPBKTERMINAL (FC)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FC

A Loopback Terminal condition occurs on an FC when a software terminal (inward) loopback is active for an MXPP_MR_2.5G or TXP_MR_2.5G card client PPM provisioned at the FC1G or FC2G line speed.

For information about troubleshooting these circuits, refer to the “[1.6 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks](#)” section on page 1-87.

Clear the LPBKTERMINAL (FC) Condition

-
- Step 1** Complete the [“Clear an MXP, TXP, or FC_MR Card Loopback Circuit” procedure on page 2-274](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.222 LPBKTERMINAL (FCMR)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FCMR

A Loopback Terminal for FCMR condition occurs when a terminal loopback is provisioned on an FC_MR-4 card.

For information about troubleshooting these circuits, refer to the [“1.6 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks” section on page 1-87](#).

Clear the LPBKTERMINAL (FCMR) Condition

-
- Step 1** Complete the [“Clear an MXP, TXP, or FC_MR Card Loopback Circuit” procedure on page 2-274](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.223 LPBKTERMINAL (G1000)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: G1000

A Loopback Terminal condition occurs when a software terminal (inward) loopback is active for a port on the reporting G-Series Ethernet card.

When a port in terminal (inward) loopback, its outgoing signal is redirected into the receive direction on the same port, and the externally received signal is ignored. On the G1000-4 card, the outgoing signal is not transmitted; it is only redirected in the receive direction.

For more information about troubleshooting Ethernet circuits, refer to the [“1.5 Troubleshooting Ethernet Circuit Paths With Loopbacks” section on page 1-69](#).



Caution

CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKTERMINAL (G1000) Condition

-
- Step 1** Complete the [“Clear Other DS-N Card, EC-1, or G1000 Card Loopbacks” procedure on page 2-274](#).

- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.224 LPBKTERMINAL (GE)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: GE

A Loopback Terminal condition for a GE port occurs when a software terminal (inward) loopback is active for an MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, or TXPP_MR_2.5G card client PPM provisioned at the ONE_GE port rate. For the TXP_MR_10E and TXP_MR_10G cards, this condition occurs when there is a facility loopback on a client PPM provisioned at the TEN_GE port rate.

For information about troubleshooting these circuits, refer to the “[1.6 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks](#)” section on page 1-87.

Clear the LPBKTERMINAL (GE) Condition

- Step 1** Complete the “[Clear an MXP, TXP, or FC_MR Card Loopback Circuit](#)” procedure on page 2-274.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.225 LPBKTERMINAL (ISC)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: ISC

A Loopback Terminal condition for an ISC port occurs when a software terminal (inward) loopback is active for a TXP_MR_2.5G client PPM provisioned at the ISC port rate.

For information about troubleshooting these circuits, refer to the “[1.6 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks](#)” section on page 1-87.

Clear the LPBKTERMINAL (ISC) Condition

- Step 1** Complete the “[Clear an MXP, TXP, or FC_MR Card Loopback Circuit](#)” procedure on page 2-274.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.226 LPBKTERMINAL (OCN)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: OCN

A Loopback Terminal condition occurs when a software terminal (inward) loopback is active for a port on the reporting card. OC-N terminal loopbacks do not typically return an AIS.

**Note**

Performing a loopback on an in-service circuit is service-affecting. If you did not perform a lockout or Force switch to protect traffic, the LPBKTERMINAL condition can also be accompanied by a more serious alarm such as LOS.

For information about troubleshooting circuits, refer to the loopback procedures in [Chapter 1, “General Troubleshooting.”](#)

Clear the LPBKTERMINAL (OCN) Condition

-
- Step 1** Complete the [“Clear an OC-N Card Facility or Terminal Loopback Circuit”](#) procedure on page 2-273.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.227 LPBKTERMINAL (TRUNK)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

A Loopback Terminal condition on MXP or TXP client or trunk cards indicates that there is an active terminal (inward) loopback on the port.

For information about troubleshooting optical circuits, refer to the [“1.4 Troubleshooting Optical Circuit Paths With Loopbacks”](#) section on page 1-47.

Clear the LPBKTERMINAL (TRUNK) Condition

-
- Step 1** Complete the [“Clear an MXP, TXP, or FC_MR Card Loopback Circuit”](#) procedure on page 2-274.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.228 LWBATVG

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: PWR

The Low Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage falls below the low power threshold. This threshold, with a default value of –44 VDC, is user-provisionable. The alarm remains raised until the voltage remains above the threshold for 120 seconds. (For information about changing this threshold, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 4, “Turn Up Node.”)

Clear the LWBATVG Alarm

-
- Step 1** The problem is external to the ONS 15454. Troubleshoot the power source supplying the battery leads.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.229 MAN-REQ

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EQPT, STSMON, VT-MON

The Manual Switch Request condition occurs when a user initiates a Manual switch request on an OC-N port. Clearing the Manual switch clears the MAN-REQ condition. You do not need to clear the switch if you want the manual switch to remain.

Clear the MAN-REQ Condition

-
- Step 1** Complete the “[Initiate a 1+1 Protection Port Manual Switch Command](#)” procedure on page 2-261.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.230 MANRESET

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

A User-Initiated Manual Reset condition occurs when you right-click a card in CTC and choose Reset. Resets performed during a software upgrade also prompt the condition. The MANRESET condition clears automatically when the card finishes resetting.

**Note**

MANRESET is an informational condition and does not require troubleshooting.

2.8.231 MANSWTOINT

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: NE-SREF

The Manual Switch To Internal Clock condition occurs when the NE timing source is manually switched to the internal timing source.

**Note**

MANSWTOINT is an informational condition and does not require troubleshooting.

2.8.232 MANSWTOPRI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Primary Reference condition occurs when the NE timing source is manually switched to the primary timing source.

**Note**

MANSWTOPRI is an informational condition and does not require troubleshooting.

2.8.233 MANSWTOSEC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Second Reference condition occurs when the NE timing source is manually switched to the second timing source.

**Note**

MANSWTOSEC is an informational condition and does not require troubleshooting.

2.8.234 MANSWTOHIRD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Third Reference condition occurs when the NE timing source is manually switched to the third timing source.

**Note**

MANSWTOHIRD is an informational condition and does not require troubleshooting.

2.8.235 MANUAL-REQ-RING

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Manual Switch Request on Ring condition occurs when a user initiates a Manual Ring command on two-fiber and four-fiber BLSR rings to switch from working to protect or protect to working.

Clear the MANUAL-REQ-RING Condition

-
- Step 1** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-267.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.236 MANUAL-REQ-SPAN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, TRUNK

The Manual Switch Request on Ring condition occurs on BLSRs when a user initiates a Manual Span command to move BLSR traffic from a working span to a protect span.

Clear the MANUAL-REQ-SPAN Condition

-
- Step 1** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-267.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.237 MEA (AIP)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: AIP

If the Mismatch of Equipment Attributes (MEA) alarm is reported against the AIP, the fuse in the AIP board blew or is missing. The MEA alarm also occurs when an old AIP board with a 2-A fuse is installed in a newer ANSI 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD).

Clear the MEA (AIP) Alarm

-
- Step 1** Complete the “[Replace the Alarm Interface Panel](#)” procedure on page 2-279.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.238 MEA (BIC)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: BIC

The Missing Equipment Attributes alarm for the backplane interface connector (BIC) indicates a compatibility issue in using high-density DS-3 cards with universal backplane interface connectors (UBIC) and an older shelf backplane. Backplane versions 15454-SA-HD and later are compatible with the UBIC with horizontal connectors (UBIC-H) and UBIC with vertical connectors (UBIC-V) that the high-density EC-1, DS-1, and DS-3 electrical connections require. The MEA alarm is raised if you attempt to install a high-density card into Slots 4, 5, 6, 12, 13, or 14 with an older noncompatible backplane installed. The card is not usable in this case. It is also raised if you attempt to use an older BIC with the newer backplane.

Clear the MEA (BIC) Alarm

- Step 1** Click the **Provisioning > Inventory** tabs to determine your backplane model. If the backplane is not a 15454-SA-HD, replace the backplane or do not attempt to use high-density DS-3 cards. [Table 2-10](#) lists the BICs that are compatible with various backplanes.

Table 2-10 BIC Compatibility Matrix

BIC Type	Part No.
BICs that work with the current and previous backplane	MANUF_EQPT_ID_BIC_A_SMB_HD_BP MANUF_EQPT_ID_BIC_B_SMB_HD_BP MANUF_EQPT_ID_BIC_A_BNC_24_HD_BP MANUF_EQPT_ID_BIC_A_BNC_48_HD_BP MANUF_EQPT_ID_BIC_B_SMB MANUF_EQPT_ID_BIC_B_SMB_ALT MANUF_EQPT_ID_BIC_B_BNC_24 MANUF_EQPT_ID_BIC_B_BNC_48
New HD BICs that work only with the new backplanes	MANUF_EQPT_ID_BIC_A_UNIV_VERT MANUF_EQPT_ID_BIC_B_UNIV_VERT MANUF_EQPT_ID_BIC_A_UNIV_HORIZ MANUF_EQPT_ID_BIC_B_UNIV_HORIZ MANUF_EQPT_ID_BIC_A_MINI_BNC_HD_BP MANUF_EQPT_ID_BIC_B_MINI_BNC_HD_BP
High-density BICs that work only with 15454-SA-HD	MANUF_EQPT_ID_BIC_A_SMB MANUF_EQPT_ID_BIC_A_SMB_ALT MANUF_EQPT_ID_BIC_A_BNC_24 MANUF_EQPT_ID_BIC_A_BNC_48

- Step 2** If you determine that your BIC type and backplane are compatible despite the MEA alarm, or if the alarm does not clear after you resolve the incompatibilities, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.239 MEA (EQPT)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The MEA alarm for equipment is reported against a card slot when the physical card inserted into a slot does not match the card type that is provisioned for that slot in CTC. The alarm also occurs when certain cards introduced in Release 3.1 or later are inserted into an older shelf assembly or when older Ethernet cards (E1000-2 and E100T-12) are used in a newer 10-Gbps-compatible shelf assembly.

Removing the incompatible cards clears the alarm.



Note

If an OC3-8 card is installed in Slots 5 to 6 and 12 to 13, it does not appear in CTC and raises an MEA.

Clear the MEA (EQPT) Alarm

Step 1 Physically verify the type of card that sits in the slot reporting the MEA alarm. In node view, click the **Inventory** tab.

Step 2 Determine whether the ONS 15454 shelf assembly is a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) or an earlier shelf assembly. Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, then you have a 15454-SA-HD shelf. If the number is not one of those listed above, then you are using an earlier shelf assembly.



Note

On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves, the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

Step 3 Verify the type of card that sits in the slot reported in the object column of the MEA row on the Alarms window by reading the name at the top of the card faceplate.

- If you have a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) and the card reporting the alarm is not an E1000-2 or E100T-12, proceed to [Step 4](#).
- If you have a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) and the card reporting the alarm is an E1000-2 or E100T-12, then that version of the Ethernet card is incompatible and must be removed. Proceed to [Step 4](#).



Note

The E1000-2-G and E100T-G cards are compatible with the newer ANSI 10-Gbps-compatible shelf assembly and are the functional equivalent of the older, noncompatible E1000-2 and E100T-12 cards. E1000-2-G and E100T-G cards can be used as replacements for E1000-2 and E100T-12 cards in a 10-Gbps-compatible shelf assembly.

- If you have an older shelf assembly and the card reporting the alarm is not a card introduced in Release 3.1 or later, which includes the OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), proceed to [Step 4](#).
- If you have an older shelf assembly and the card reporting the alarm is a card introduced in Release 3.1 or later, which includes the OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), the reporting card is incompatible with the shelf assembly and must be removed. Proceed to [Step 4](#).

- Step 4** If you prefer the card type depicted by CTC, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the reporting card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 5** If you prefer the card that physically occupies the slot but the card is not in service, has no circuits mapped to it, and is not part of a protection group, put the cursor over the provisioned card in CTC and right-click to choose **Delete Card**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

**Note**

If the card is in service, has a circuit mapped to it, is paired in a working protection scheme, has DCC communications turned on, or is used as a timing reference, CTC does not allow you to delete the card.

- Step 6** If any ports on the card are in service, place them out of service (OOS,MT):

**Caution**

Before placing ports out of service, ensure that live traffic is not present.

- a. Double-click the reporting card to display the card view.
- b. Click the **Provisioning** tab.
- c. Click the admin state of any in-service ports.
- d. Choose **OOS,MT** to take the ports out of service.

- Step 7** If a circuit has been mapped to the card, complete the [“Delete a Circuit” procedure on page 2-272](#).

**Caution**

Before deleting the circuit, ensure that live traffic is not present.

- Step 8** If the card is paired in a protection scheme, delete the protection group:

- a. Click the **Provisioning > Protection** tabs.
- b. Choose the protection group of the reporting card.
- c. Click **Delete**.

- Step 9** Right-click the card reporting the alarm.

- Step 10** Choose **Delete**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

- Step 11** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.240 MEA (FAN)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: FAN

The MEA alarm is reported against the fan-tray assembly when a newer fan-tray assembly (15454-FTA3) with a 5-A fuse is used with an older shelf assembly or when an older fan-tray assembly with a 2-A fuse is used with a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) that contains cards introduced in Release 3.1 or later. If a 10-Gbps-compatible shelf assembly contains only cards introduced before Release 3.1, then an older fan-tray assembly (15454-FTA-2) can be used and does not report an MEA alarm.

Clear the MEA (FAN) Alarm

-
- Step 1** Determine whether the shelf assembly is a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) or an earlier shelf assembly. In node view, click the **Inventory** tab.
- Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, you have a 15454-SA-HD shelf.
- Under the HW Part # column, if the number is not one of those listed above, then you are using an earlier shelf assembly.
- Step 2** If you have a 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD), the alarm indicates that an older incompatible fan-tray assembly is installed in the shelf assembly. Obtain a newer fan-tray assembly (15454-FTA3) with a 5-A fuse and complete the [“Replace the Fan-Tray Assembly” procedure on page 2-277](#).
- Step 3** If you are using an earlier shelf assembly, the alarm indicates that you are using a newer fan-tray assembly (15454-FTA3), which is incompatible with the earlier version of the shelf assembly. Obtain an earlier version of the fan-tray assembly (15454-FTA2) and complete the [“Replace the Fan-Tray Assembly” procedure on page 2-277](#).
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.241 MEA (PPM)

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: PPM

The Missing Equipment Attributes alarm for the PPM is raised on DWDM cards when the PPM is misprovisioned or unsupported. It can occur when you plug in a PPM without first provisioning it, or when you provision the PPM for a wavelength that is explicitly not the first tunable wavelength.

Clear the MEA (PPM) Alarm

-
- Step 1** To provision the PPM, you must first create it in CTC. To do this, complete the following steps:
- Double-click the MXP or TXP MR card to display the card view.
 - Click the **Provisioning > Pluggable Port Modules** tabs. (If you already see the PPM listed in the Pluggable Port Modules Area, go to [Step 2](#).)
 - Under the Pluggable Port Modules area, click **Create**.
 - In the Create PPM dialog box, choose the MXP or TXP card PPM number from the drop-down list (for example, PPM 1).
 - Choose the PPM type from the second drop-down list, for example PPM (1 Port).
 - Click **OK**.
- Step 2** After you have created the PPM, or if you see it listed in the Pluggable Port Modules area but not in the Selected PPM area, choose the port rate:
- Under the Selected PPM area, click **Create**.
 - In the Create Port dialog box, choose the port (for example, 1-1) from the drop-down list.
 - Choose the correct port type from the drop-down list. (For more information about selecting PPM port types, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*, Chapter 10, “Change Card Settings.”)
 - Click **OK**.
- Step 3** If you see the port listed in the Pluggable Port Modules area and the Selected PPM, the MEA indicates that the incorrect port rate was selected. Click the port in the Selected PPM area and click **Delete**.
- Step 4** Complete [Step 2](#) to correctly provision the port rate.
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.242 MEM-GONE

- Default Severity: Major (MJ), Service Affecting (SA)
- Logical Object: EQPT

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TCC2/TCC2P card. CTC does not function properly until the alarm clears. The alarm clears when additional memory becomes available.



Note

The alarm does not require user intervention. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.243 MEM-LOW

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC2/TCC2P card. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the TCC2/TCC2P is exceeded, CTC ceases to function.

**Note**

The alarm does not require user intervention. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.244 MFGMEM

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: AICI-AEP, AICI-AIE, AIP, BPLANE, EQPT, FAN, PPM

The Manufacturing Data Memory Failure alarm occurs when the EEPROM fails on a card or component, or when the TCC2/TCC2P card cannot read this memory. EEPROM stores manufacturing data that a system TCC2/TCC2P uses to determine system compatibility and shelf inventory status. Unavailability of this information can cause minor problems. The AIP EEPROM also stores the system MAC address. If the MFGMEM alarm indicates EEPROM failure on these panels, IP connectivity could be disrupted and the system icon is grayed out in CTC network view.

**Tip**

When you lose LAN connectivity with an ONS 15454 due to an MFGMEM alarm on the AIP, you can reestablish node management by disconnecting the Ethernet cable from the panel and connecting it to the active TCC2/TCC2P LAN port.

Clear the MFGMEM Alarm

-
- Step 1** Complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-270](#).
- Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
- Step 2** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card” procedure on page 2-270](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#).
- Step 3** If the MFGMEM alarm continues to report after replacing the TCC2/TCC2Ps, the problem is with the EEPROM.
- Step 4** If the MFGMEM is reported from the fan-tray assembly, obtain a fan-tray assembly and complete the [“Replace the Fan-Tray Assembly” procedure on page 2-277](#).
- Step 5** If the MFGMEM is reported from the AIP, the backplane, or the alarm persists after the fan-tray assembly is replaced, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.8.245 NO-CONFIG

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The No Startup Configuration condition applies to ML-Series Ethernet cards and occurs when no startup configuration file has been downloaded to the TCC2/TCC2P, whether or not you preprovision the card slot. This alarm is to be expected during provisioning. When the startup configuration file is copied to the active TCC2/TCC2P, the alarm clears.



Note

For more information about the ML-Series Ethernet cards, refer to the *<I>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the NO-CONFIG Condition

-
- Step 1** Create a startup configuration for the card in Cisco IOS.
- Follow the card provisioning instructions in the *<I>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.
- Step 2** Upload the configuration file to the TCC2/TCC2P:
- In node view, right-click the ML-Series card graphic.
 - Choose **IOS Startup Config** from the shortcut menu.
 - Click **Local > TCC** and navigate to the file location.
- Step 3** Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-268.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.246 NOT-AUTHENTICATED

- Default Severity: Minor (MN), Non-Service-Affecting (NSA)
- Logical Object: SYSTEM

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when it fails to log into a node. This alarm only displays in CTC where the login failure occurred. This alarm differs from the “[INTRUSION-PSWD](#)” alarm on page 2-129 in that INTRUSION-PSWD occurs when a user exceeds the login failures threshold.



Note

NOT-AUTHENTICATED is an informational alarm and is resolved when CTC successfully logs into the node.

2.8.247 OCHNC-INC

The OCHNC-INC condition is not used in this platform in this release. It is reserved for future development.

2.8.248 ODUK-1-AIS-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK-1-AIS-PM is a secondary condition raised on MXP card trunk signals when they experience an LOS (2R). Although the ODUK-1-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

A single ODUK-x-AIS-PM can occur when one remote-node client signal is lost; multiple ODK-x-AIS-PMs can occur (ODUK-1-AIS-PM, ODUK-2-AIS-PM, ODUK-3-AIS-PM, ODUK-4-AIS-PM) if more than one remote-node client is lost. If the entire trunk signal is lost, LOS (TRUNK) occurs and demotes any LOS (2R) alarms.

Clear the ODUK-1-AIS-PM Condition

-
- Step 1** Look for and clear the LOS (2R) alarm on remote-node client. This should clear the ODUK-1-AIS-PM condition on trunk.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.249 ODUK-2-AIS-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK-2-AIS-PM is a secondary condition raised on MXP card trunk signals when they experience an LOS (2R). Although the ODUK-2-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

A single ODUK-x-AIS-PM can occur when one remote-node client signal is lost; multiple ODK-x-AIS-PMs can occur (ODUK-1-AIS-PM, ODUK-2-AIS-PM, ODUK-3-AIS-PM, ODUK-4-AIS-PM) if more than one remote-node client is lost. If the entire trunk signal is lost, LOS (TRUNK) occurs and demotes any LOS (2R) alarms.

Clear the ODUK-2-AIS-PM Condition

-
- Step 1** Complete the [“Clear the ODUK-1-AIS-PM Condition” procedure on page 2-187](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.250 ODUK-3-AIS-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK-3-AIS-PM is a secondary condition raised on MXP card trunk signals when they experience an LOS (2R). Although the ODUK-3-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

A single ODUK-x-AIS-PM can occur when one remote-node client signal is lost; multiple ODK-x-AIS-PMs can occur (ODUK-1-AIS-PM, ODUK-2-AIS-PM, ODUK-3-AIS-PM, ODUK-4-AIS-PM) if more than one remote-node client is lost. If the entire trunk signal is lost, LOS (TRUNK) occurs and demotes any LOS (2R) alarms.

Clear the ODUK-3-AIS-PM Condition

-
- Step 1** Complete the “[Clear the ODUK-1-AIS-PM Condition](#)” procedure on page 2-187.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.251 ODUK-4-AIS-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK-4-AIS-PM is a secondary condition raised on MXP card trunk signals when they experience an LOS (2R). Although the ODUK-4-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

A single ODUK-x-AIS-PM can occur when one remote-node client signal is lost; multiple ODK-x-AIS-PMs can occur (ODUK-1-AIS-PM, ODUK-2-AIS-PM, ODUK-3-AIS-PM, ODUK-4-AIS-PM) if more than one remote-node client is lost. If the entire trunk signal is lost, LOS (TRUNK) occurs and demotes any LOS (2R) alarms.

Clear the ODUK-4-AIS-PM Condition

-
- Step 1** Complete the “[Clear the ODUK-1-AIS-PM Condition](#)” procedure on page 2-187.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.252 ODUK-AIS-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Optical Data Unit (ODUK) AIS Path Monitoring (PM) condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. ODUK-AIS-PM is a secondary condition that indicates a more serious condition such as the “LOS (OCN)” alarm on page 2-153 occurring downstream. The ODUK-AIS-PM condition is reported in the path monitoring area of the optical data unit wrapper overhead. ODUK-AIS-PM is caused by the upstream 2.8.255 ODUK-OCI-PM, page 2-190.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the ODUK-AIS-PM Condition

-
- Step 1** Determine whether upstream nodes and equipment have alarms, especially the “LOS (OCN)” alarm on page 2-153, or OOS ports.
- Step 2** Clear the upstream alarms using the applicable procedures in this chapter.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.253 ODUK-BDI-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Backward Defect Indicator (BDI) PM condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. It indicates that there is a path termination error upstream in the data. The error is read as a BDI bit in the path monitoring area of the digital wrapper overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP cards or MXP cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the ODUK-BDI-PM Condition

-
- Step 1** Complete the “Clear the OTUK-BDI Condition” procedure on page 2-197.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.254 ODUK-LCK-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)

- Logical Object: TRUNK

The ODUK Locked Defect (LCK) PM condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. ODUK-LCK-PM indicates that a signal is being sent downstream to indicate that the upstream connection is locked, preventing the signal from being passed. The lock is indicated by the STAT bit in the path overhead monitoring fields of the optical transport unit overhead of the digital wrapper.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the ODUK-LCK-PM Condition

-
- Step 1** Unlock the upstream node signal.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.255 ODUK-OCI-PM

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Open Connection Indication (OCI) PM condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. It indicates that the upstream signal is not connected to a trail termination source. The error is read as a STAT bit in the path monitoring area of the digital wrapper overhead. ODUK-OCI-PM causes an [2.8.254 ODUK-LCK-PM, page 2-189](#), downstream.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the ODUK-OCI-PM Condition

-
- Step 1** Verify the fiber connectivity at nodes upstream.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.256 ODUK-SD-PM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: TRUNK

The ODUK Signal Degrade (SD) PM condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. ODUK-SD-PM indicates that incoming signal quality is poor, but the incoming line bit error rate (BER) has not passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the ODUK-SD-PM Condition

-
- Step 1** Complete the “[Clear the SD-L Condition](#)” procedure on page 2-220.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.257 ODUK-SF-PM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Signal Fail (SF) PM condition (ODUK-SD-PM) applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. ODUK-SF-PM indicates that incoming signal quality is poor and the incoming line BER has passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the ODUK-SF-PM Condition

-
- Step 1** Complete the “[Clear the SF \(DS1, DS3\) Condition](#)” procedure on page 2-222.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.258 ODUK-TIM-PM

- Default Severity: Major (MJ), Service-Affecting (NSA)
- Logical Object: TRUNK

The ODUK Trace Identifier Mismatch (TIM) PM condition applies to the path monitoring area of the OTN overhead for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. The condition occurs when there is a trace identifier mismatch in the data stream. ODUK-TIM-PM causes an [2.8.253 ODUK-BDI-PM, page 2-189](#), downstream.

The ODUK-TIM-PM condition applies to TX cards and MXP cards when ITU-T G.709 monitoring is enabled for the cards. It indicates that there is an error upstream in the optical transport unit overhead of the digital wrapper.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the ODUK-TIM-PM Condition

-
- Step 1** Complete the [“Clear the TIM-P Alarm” procedure on page 2-243](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.259 OOU-TPT

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSTRM, VT-TERM

The Out of Use Transport Failure alarm is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) This condition is raised when a member circuit in a VCAT is unused, such as when it is removed by SW-LCAS. It occurs in conjunction with the [“VCG-DEG” condition on page 2-253](#).

Clear the OOT-TPT Condition

-
- Step 1** Complete the [“Clear the VCG-DEG Condition” procedure on page 2-253](#). Clearing that condition clears this condition as well.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.260 OPTNTWMIS

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The Optical Network Type Mismatch alarm is raised when DWDM nodes are not configured for the same type of network, either MetroCore or MetroAccess. All DWDM nodes on the same network must be configured for the same network type because APC and ANS behave differently on each of these network types. For more information about APC and ANS, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

When the OPTNTWMIS occurs, the “APC-DISABLED” alarm on page 2-33 could also be raised.

Clear the OPTNTWMIS Alarm

-
- Step 1** In node view of the alarmed node, click the **Provisioning > WDM-ANS > Provisioning** tabs.
- Step 2** Choose the correct option from the Network Type list box, and click **Apply**.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.261 OPWR-HDEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power High Degrade alarm occurs on all DWDM ports that use a setpoint, including the OPT-BST and OPT-PRE card AOTS ports in control power mode; the 32DMX, 32DMX-O, 32MUX-O, and 32WSS card OCH ports, and the OSC-CSM and OSCM OSC-TX ports.

The alarm generally indicates that an internal signal transmission problem prevents the signal output power from maintaining its setpoint and the signal has crossed the high degrade threshold. For 32DMX, 32DMX-O, 32MUX-O, and 32WSS OCH ports and OSC-CSM and OSCM OSC-TX ports, OPWR-HDEG indicates that the card has a VOA control circuit failure affecting its attenuation capability. The alarmed card should be replaced at the next opportunity.

Clear the OPWR-HDEG Alarm

-
- Step 1** Verify fiber continuity to the port.



Note To verify fiber continuity, follow site practices.

- Step 2** If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.
- Step 3** Verify that the power read by photodiode on the port is within the expected range foreseen by MetroPlanner. The application generates a spreadsheet of values containing this information.
- Step 4** If the optical power level is within specifications, check the opwrMin threshold. Consult the *Cisco MetroPlanner DWDM Operations Guide* and decide what value to use for modifying the power level:
- Double-click the card to display the card view.
 - Display the optical thresholds by clicking the following tabs:

- OPT-BST Provisioning > Opt. Ampli. Line > Optics Thresholds tab
- OPT-PRE Provisioning > Opt. Ampli. Line > Optics Thresholds tab
- AD-xC Provisioning > Optical Chn> Optics Thresholds tab
- AD-xB Provisioning > Optical Band > Optics Thresholds tab
- 32DMX or 32DMX-O Provisioning > Optical Chn > Optics Thresholds tab
- 32MUX Provisioning > Optical Chn > Optics Thresholds tab
- 32WSS Provisioning > Optical Chn: Optical Connector *x* > Optics Thresholds tab
- OSCM or OSC-CSM Provisioning > Optical Line > Optics Thresholds tab

Step 5 If the received optical power level is within specifications, consult the *Cisco MetroPlanner DWDM Operations Guide* to determine the correct levels and check the opwrMin threshold. If necessary, modify the value as required.

Step 6 If the optical power is outside of the expected range, verify that all involved optical signal sources, namely the TXP or MXP trunk port or an ITU-T line card, are in IS admin state by clicking the correct tab:

- MXPP_MR_2.5G Provisioning > Line > OC48 tab
- MXP_2.5G_10E Provisioning > Line > Trunk tab
- MXP_2.5G_10G Provisioning > Line > SONET tab
- MXP_MR_2.5G Provisioning > Line > OC48 tab
- TXPP_MR_2.5G Provisioning > Line > OC48 tab
- TXP_MR_10E Provisioning > Line > SONET tab
- TXP_MR_10G Provisioning > Line > SONET tab
- TXP_MR_2.5G Provisioning > Line > SONET tab

If it is not IS-NR, choose **IS** from the admin state drop-down list. This creates the IS-NR service state.

Step 7 If the port is in IS-NR service state but its output power is outside of the specifications, complete the “Clear the LOS-P (OCH) Alarm” procedure on page 2-159.

Step 8 If the signal source is IS and within expected range, come back to the unit reporting OPWR-HDEG and clean all connected fiber in the same line direction as the reported alarm according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”



Note Unplugging fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the procedures in the “2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260. For more detailed protection switching information, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

Step 9 Repeat Steps 1 to 8 for any other port on the card reporting the OPWR-HDEG alarm.

Step 10 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 11 If no other alarms exist that could be the source of the OPWR-HDEG, or if clearing an alarm did not clear the alarm, place all of the card ports in OOS,DSBLD admin state.

Step 12 Complete the “Physically Replace a Traffic Card” procedure on page 2-271 for the reporting card.



Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform a traffic switch if possible.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database apart from restoring the card's port to the IS,AINS admin state.

Step 13 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.262 OPWR-HFAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Failure alarm occurs on an DWDM OPT-BST or OPT-PRE amplifier card AOTS port if the transmitted power exceeds the high fail threshold. This alarm is raised only in control power working mode. The alarmed card should be replaced at the next opportunity.

Clear the OPWR-HFAIL Alarm

Step 1 Complete the “[Clear the OPWR-HDEG Alarm](#)” procedure on page 2-193.

Step 2 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.263 OPWR-LDEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Low Degrade alarm occurs on all DWDM ports that use a setpoint, including the OPT-BST and OPT-PRE card AOTS ports in control power mode; the 32DMX, 32DMX-O, 32MUX-O, and 32WSS card OCH ports; and the OSC-CSM and OSCM card OSC-TX ports.

The alarm generally indicates that an internal signal transmission problem prevents the signal output power from maintaining its setpoint and the signal has crossed the low degrade threshold. For the 32DMX, 32DMX-O, 32MUX-O, and 32WSS card OCH ports and the OSC-CSM and OSCM card OSC-TX ports, OPWR-HDEG indicates that the card has a VOA control circuit failure affecting its attenuation capability. The alarmed card should be replaced at the next opportunity.

Clear the OPWR-LDEG Alarm

Step 1 Complete the “[Clear the OPWR-HDEG Alarm](#)” procedure on page 2-193.

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.264 OPWR-LFAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Failure alarm applies to DWDM OPT-BS T and OPT-PRE amplifier AOTS ports. It also applies to AD-1B-xx.x, AD-4B-xx.x, AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, OPT-PRE, OPT-BST, 32MUX-O, 32DMX, 32DMX-O, 32DMX, 32WSS, and OSC-CSM transmit (TX) ports. The alarm is raised when monitored input power crosses the low fail threshold.

For the AD-1B-xx.x, AD-4B-xx.x, AD-1C-xx.x, AD-2C-xx.x, and AD-4C-xx.x card OCH ports and the 32MUX-O, 32DMX, 32DMX-O; 32WSS, OSCM, and OSC-CSM cards, OPWR-LFAIL indicates that the card has a VOA control circuit failure that affects its attenuation capability.

Clear the OPWR-LFAIL Alarm

- Step 1** Complete the “[Clear the OPWR-HDEG Alarm](#)” procedure on page 2-193.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.265 OSRION

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OTS

The Optical Safety Remote Interlock On condition is raised for OPT-PRE and OPT-BST amplifier cards when OSRI is set to ON. The condition does not correlate with the “[OPWR-LFAIL](#)” alarm on page 2-196 also reported on the same port.

Clear the OSRION Condition

- Step 1** Turn the OSRI off:
- Double-click the card to display the card view.
 - Click the **Maintenance > ALS** tabs.
 - In the OSRI column, choose **OFF** from the drop-down list.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.266 OTUK-AIS

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Optical Transport Unit (OTUK) AIS condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. OTUK-AIS is a secondary condition that indicates a more serious condition, such as the “LOS (OCN)” alarm on page 2-153, is occurring downstream. OTUK-AIS is reported in the optical transport unit overhead of the digital wrapper.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the OTUK-AIS Condition

-
- Step 1** Complete the “Clear the AIS Condition” procedure on page 2-31.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.267 OTUK-BDI

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The OTUK BDI condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. OTUK-BDI is indicated by the BDI bit in the section monitoring overhead. The alarm occurs when there is an SF condition upstream. OTUK-BDI is triggered by the “OTUK-TIM” condition on page 2-200.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the OTUK-BDI Condition

-
- Step 1** Determine whether upstream nodes have the “OTUK-AIS” condition on page 2-197.
- Step 2** In the upstream node, click the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card in node view to display the card view.
- Step 3** Click the **Provisioning > OTN > Trail Trace Identifier** tabs.
- Step 4** Compare the Current Transmit String with the Current Expected String in the downstream node. (Verify the Current Expected String by making the same navigations in another CTC session to the downstream node.)

- Step 5** If the two do not match, modify the Current Expected String.
- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.268 OTUK-IAE

Default Severity: [Minor (MN), Non-Service-Affecting (NSA)]

Logical Object: TRUNK

The OTUK Section-Monitoring Incoming Alignment Error (IAE) alarm occurs on TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards and the trunk connection is present. This alarm is raised on the near-end node to indicate that the far-end node it has detected errors in the received OTU frames, but they might not be bad enough to cause an “OTUK-LOF” alarm on page 2-199.

The IAE bit in the section overhead allows the ingress point (in this case, the far-end node) to inform its corresponding egress (near-end) point that the alignment error is detected on the incoming signal OTU frame alignment errors from NE. The error is an out-of-frame (OOF) alignment, in which the optical transport unit overhead frame alignment (FAS) area is errored for more than five frames. If the OOF condition persists for 3ms, OTUK-LOF is raised.



Note

For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the OTUK-IAE Alarm

- Step 1** At the near-end and far-end node, use site practices to clean transmitting fiber on near-end node's reporting port and receiving fiber on correspondent far-end port. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”
- Step 2** If the OTUK-IAE alarm does not clear, look for other OTU-related alarm, such as the “OTUK-LOF” alarm on page 2-199, at the far-end node and resolve it using the appropriate procedure in this guide.
- Step 3** If the OTUK-IAE alarm does not clear, use an OTN test set such as the Agilent OmniBerOTN tester to check near-end transmitting signal quality.
- For specific procedures to use the test set equipment, consult the manufacturer.
- Step 4** If the source of the alarm is not found, verify the two nodes' timing source. To do this, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 10, “Change Node Settings,” DLP-A195 “Verify Timing in a Reduced Ring.”
- For specific procedures to use the test set equipment, consult the manufacturer.
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.269 OTUK-LOF

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: TRUNK

The OTUK-LOF alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled for the cards. The alarm indicates that the card has lost frame delineation on the input data. Loss of frame occurs when the optical transport unit overhead frame alignment (FAS) area is errored for more than five frames and that the error persists more than three milliseconds.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card of MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the OTUK-LOF Alarm

-
- Step 1** Complete the “[Clear the LOF \(OCN\) Alarm](#)” procedure on page 2-143.
- Step 2** If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.270 OTUK-SD

- Default Severity: Not Alarmed (NA) Non-Service Affecting (NSA)
- Logical Object: TRUNK

The OTUK-SD condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. The condition indicates that incoming signal quality is poor, but the incoming line BER has not passed the fail threshold. The BER problem is indicated in the optical transport unit frame overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and MXP_2.5G_10G cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the OTUK-SD Condition

-
- Step 1** Complete the “[Clear the SD-L Condition](#)” procedure on page 2-220.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.271 OTUK-SF

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The OTUK-SF condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. The condition indicates that incoming signal quality is poor and that the BER for the incoming line has passed the fail threshold. The BER problem is indicated in the optical transport unit frame overhead.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP and MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the OTUK-SF Condition

-
- Step 1** Complete the “[Clear the SD-L Condition](#)” procedure on page 2-220.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.272 OTUK-TIM

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: TRUNK

The OTUK-TIM alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled and section trace mode is set to manual. The alarm indicates that the expected TT1 string does not match the received TTI string in the optical transport unit overhead of the digital wrapper. OTUK-TIM triggers an “[ODUK-BDI-PM](#)” condition on page 2-189.

ITU-T G.709 monitoring refers to a digital data wrapper that is transparent across networking standards (such as SONET) and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 8, “Monitor Performance.”

Clear the OTUK-TIM Condition

-
- Step 1** Complete the “[Clear the TIM-P Alarm](#)” procedure on page 2-243.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.273 OUT-OF-SYNC

- Default Severity: Major (MJ), Service Affecting (SA)
- Logical Objects: FC, GE, ISC, TRUNK

The Ethernet Out of Synchronization condition occurs on TXP_MR_2.5 and TXPP_MR_2.5 cards when the PPM port is not correctly configured for the Gigabit Ethernet payload rate.

Clear the OUT-OF-SYNC Condition

-
- Step 1** Double-click the alarmed card to display the card view.
- Step 2** Delete the provisioning for the PPM:
- a. Click the PPM in the Selected PPM area.
 - b. Click **Delete**.
- Step 3** Recreate the PPM provisioning using the correct data rate:
- a. Click **Create**.
 - b. In the Port Type drop-down list, choose **ONE_GE**.
 - c. Click **OK**.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.274 PARAM-MISM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Plug-in Module Range Settings Mismatch condition is raised for OPT-BST and OPT-PRE amplifier cards, optical add-drop multiplexer (OADM) cards (AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, and AD-4B-xx.x), multiplexer cards (32MUX-O and 32WSS), and demultiplexer cards (32DMX-O and 32DMX) when the parameter range values stored on the card are different from the parameters stored in TCC2/TCC2P database. The condition is not user-serviceable. Log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.275 PDI-P

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

PDI-P is a set of application-specific codes indicating a signal label mismatch failure (SLMF) in the ONS 15454 STS path overhead. The alarm indicates to downstream equipment that there is a defect in one or more of the directly mapped payloads contained in that STS synchronous payload envelope (SPE). For example, the mismatch could occur in the overhead to the path selector in a downstream node configured as part of a path protection. The PDI-P codes appear in the STS Signal Label (C2 byte).

An SLMF often occurs when the payload (for example, ATM) does not match what the signal label is reporting. The “AIS” condition on page 2-30 often accompanies a PDI-P condition. If the PDI-P is the only condition reported with the AIS, clearing PDI-P clears the AIS. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid condition.

A PDI-P condition reported on an OC-N port supporting a G1000-4 card circuit could result from the end-to-end Ethernet link integrity feature of the G1000-4 card. If the link integrity is the cause of the path defect, it is typically accompanied by the “TPTFAIL (G1000)” alarm on page 2-245 or the “CARLOSS (G1000)” alarm on page 2-58 reported against one or both Ethernet ports terminating the circuit. If this is the case, clear the TPTFAIL and CARLOSS alarms to resolve the PDI-P condition.

A PDI-P condition reported on an OC-N port supporting an ML-Series card circuit could result from the end-to-end Ethernet link integrity feature of the ML-Series card. If the link integrity is the cause, it is typically accompanied by the “TPTFAIL (ML100T, ML1000)” alarm on page 2-245 reported against one or both packet-over-SONET (POS) ports terminating the circuit. If TPTFAIL is reported against one or both of the POS ports, troubleshooting the accompanying alarm clears the PDI-P condition. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for more information about ML-Series cards.

**Warning**

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293

**Warning**

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056

**Warning**

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

Clear the PDI-P Condition

-
- Step 1** Verify that all circuits terminating in the reporting card are DISCOVERED:
- a. Click the **Circuits** tab.
 - b. Verify that the Status column lists the circuit as active.
 - c. If the Status column lists the circuit as PARTIAL, wait 10 minutes for the ONS 15454 to initialize fully. If the PARTIAL status does not change after full initialization, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).
- Step 2** After determining that the circuit is DISCOVERED, ensure that the signal source to the card reporting the alarm is working.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If traffic is affected, complete the [“Delete a Circuit” procedure on page 2-272](#).



Caution Deleting a circuit can affect existing traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* Chapter 6, “Create Circuits and Tunnels,” for detailed procedures to create circuits.

Step 5 If circuit deletion and recreation does not clear the condition, verify that there is no problem stemming from the remote-node OC-N card providing STS payload to the reporting card.

Step 6 If the condition does not clear, confirm the cross-connect between the OC-N card and the reporting card.

Step 7 If the condition does not clear, clean the remote-node optical fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

Step 8 If the condition does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the optical/electrical cards.



Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 9 If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.276 PEER-NORESPONSE

- Default Severity: Major (MJ), Non-Service Affecting (NSA)
- Logical Object: EQPT

The switch agent raises a Peer Card Not Responding alarm if either traffic card in a protection group does not receive a response to the peer status request message. PEER-NORESPONSE is a software failure and occurs at the task level, as opposed to a communication failure, which is a hardware failure between peer cards.

Clear the PEER-NORESPONSE Alarm

Step 1 Complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for the reporting card. For the LED behavior, see the [“2.10.2 Typical Traffic Card LED Activity During Reset” section on page 2-258](#).

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.277 PLM-P

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: STSMON, STSTRM

A Payload Label Mismatch Path alarm indicates that signal does not match its label. The condition occurs due to a problematic C2 byte value in the SONET path overhead. The alarm is raised if all of the following conditions are met:

- The received C2 byte is not 0x00 (unequipped).
- The received C2 byte is not a PDI value.
- The received C2 does not match the expected C2.
- The expected C2 byte is not 0x01 (equipped, unspecified).
- The received C2 byte is not 0x01 (equipped, unspecified).

For example, on nodes equipped with CTC Software R4.1 and earlier, this alarm could occur when you have a DS3XM-6 card connected to a DS-3 card instead of a DS-1 card. The DS3XM-6 card expects a C2 label byte value of 01. A DS-1 card transmits this value, but a DS-3 card transmits a value of 04. The mismatch between the sent and expected values causes the PLM-P alarm.



Warning

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293.



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

Clear the PLM-P Alarm

- Step 1** Complete the [“Clear the PDI-P Condition” procedure on page 2-202](#).



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.278 PLM-V

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: VT-TERM

A Payload Label Mismatch VT Layer alarm indicates that the content of the V5 byte in the SONET overhead is inconsistent or invalid. PLM-V occurs when ONS 15454s interoperate with equipment that performs bit-synchronous mapping for DS-1. The ONS 15454 uses asynchronous mapping.

Clear the PLM-V Alarm

-
- Step 1** Verify that your signal source matches the signal allowed by the traffic card. For example, the traffic card does not allow VT6 or VT9 mapping.
- Step 2** If the signal source matches the card, verify that the SONET VT path originator is sending the correct VT label value. You can find the SONET VT path originator using circuit provisioning steps.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.279 PORT-ADD-PWR-DEG-HI

The Add Port Power High Degrade alarm is not used in this platform in this release in this release. It is reserved for future development.

2.8.280 PORT-ADD-PWR-DEG-LOW

The Add Port Power Low Degrade alarm is not used in this platform in this release. It is reserved for future development.

2.8.281 PORT-ADD-PWR-FAIL-HI

The Add Port Power High Fail alarm is not used in this platform in this release. It is reserved for future development.

2.8.282 PORT-ADD-PWR-FAIL-LOW

- Default Severity: Critical (CR), Non-Service Affecting (NSA)
- Logical Object: OCH

The Add Port Power Low Fail alarm occurs on a 32WSS ADD port if an internal signal transmission crosses the low fail threshold and prevents the signal output power from reaching its setpoint. This alarm indicates that the card has a VOA control circuit failure, which affects the card automatic signal attenuation. The alarmed card should be replaced at the next opportunity.

Clear the PORT-ADD-PWR-FAIL-LOW Alarm

Step 1 Verify fiber continuity to the port.



Note To verify fiber continuity, follow site practices.

Step 2 If the cabling is okay, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

Step 3 Verify that the received power (opwrMin) is within the expected range shown in Cisco MetroPlanner. To check the level:

- a. Double-click the card to display the card view.
- b. Display the optical thresholds by clicking the 32WSS **Provisioning > Optical Chn: Optical Connector x > Optics Thresholds** tab.

Step 4 If the optical power level is within specifications, check the opwrMin threshold and consult the *Cisco MetroPlanner DWDM Operations Guide* to determine the correct value. Modify the value as necessary.

Step 5 If the power value is outside the expected range verify that the trunk port of a TXP or MXP card connected to ADD-RX port is in IS-NR service state by clicking the correct tab:

- MXPP_MR_2.5G **Provisioning > Line > OC48** tab
- MXP_2.5G_10E **Provisioning > Line > Trunk** tab
- MXP_2.5G_10G **Provisioning > Line > SONET** tab
- MXP_MR_2.5G **Provisioning > Line > OC48** tab
- TXPP_MR_2.5G **Provisioning > Line > OC48** tab
- TXP_MR_10E **Provisioning > Line > SONET** tab
- TXP_MR_10G **Provisioning > Line > SONET** tab
- TXP_MR_2.5G **Provisioning > Line > SONET** tab

If it is not IS-NR, choose **IS** from the admin state drop-down list. This creates the IS-NR service state.

Step 6 If the port is in IS-NR service state but its output power is outside of the specifications, complete the “Clear the LOS-P (OCH) Alarm” procedure on page 2-159.

Step 7 If the signal source is IS-NR and within expected range, come back to the port reporting the PORT-ADD-PWR-FAIL-LOW alarm and clean the fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

Step 8 Repeat Steps 1 through 7 for any other port on the card reporting the alarm.

Step 9 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 10 If no other alarms exist that could be the source of the PORT-ADD-PWR-FAIL-LOW, or if this procedure did not clear the alarm, place all of the card ports in OOS,DSBLD admin state.

Step 11 Complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the reporting card.



Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform a traffic switch if possible. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for short-version procedures. For more detailed protection switching information, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”



Note When you replace a card with an identical type of card, you do not need to make any changes to the database apart from restoring the card's port to the IS,AINS admin state.

Step 12 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.283 PORT-MISMATCH

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FCMR

The Pluggable Port Mismatch alarm applies to ML-Series Ethernet (traffic) card and TXP card SFP connectors. The alarm indicates that the provisioned payload for the connector does not match the SFP configuration.

The error must be resolved in the Cisco IOS configuration. PORT-MISMATCH cannot be resolved in CTC. For information about provisioning the ML-Series Ethernet cards from the Cisco IOS interface, refer to the *<I_Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.8.284 PRC-DUPID

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: NE, OCN

The Procedural Error Duplicate Node ID alarm indicates that two identical node IDs exist in the same ring. The ONS 15454 requires each node in the ring to have a unique node ID.

Clear the PRC-DUPID Alarm

-
- Step 1** Log into a node on the ring.
- Step 2** Find the node ID by completing the “[Identify a BLSR Ring Name or Node ID Number](#)” procedure on page 2-259.
- Step 3** Repeat [Step 2](#) for all the nodes on the ring.

- Step 4** If two nodes have an identical node ID number, complete the [“Change a BLSR Node ID Number” procedure on page 2-259](#) so that each node ID is unique.
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.285 PROTNA

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Protection Unit Not Available alarm is caused by an OOS protection card when a TCC2/TCC2P or XC10G cross-connect card that has been provisioned as part of a protection group is not available. Unavailable protection can occur when a card is reset, but the alarm clears as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

Clear the PROTNA Alarm

- Step 1** If the PROTNA alarm occurs and does not clear, and if it is raised against a controller or cross-connect card, ensure that there is a redundant TCC2/TCC2P card installed and provisioned in the chassis.
- Step 2** If the alarm is raised against a line card, verify that the ports have been taken out of service (OOS,MT):
- In CTC, double-click the reporting card to display the card view (if the card is not an XC10G cross-connect card).
 - Click the **Provisioning** tab.
 - Click the admin state of any in-service (IS) ports.
 - Choose **OOS,MT** to take the ports out of service.
- Step 3** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for the reporting card. For the LED behavior, see the [“2.10.2 Typical Traffic Card LED Activity During Reset” section on page 2-258](#).
- Step 4** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 5** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-270](#) for the reporting card.
- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.286 PTIM

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Payload Type Identifier Mismatch alarm occurs when there is a mismatch between the way the ITU-T G.709 option is configured on MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card at each end of the optical span.

Clear the PTIM Alarm

-
- Step 1** Double-click the alarmed MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card to display the card view.
- Step 2** Click the **Provisioning > OTN > OTN Lines** tabs.
- Step 3** Ensure that the G.709 OTN check box is checked. If not, check it and click **Apply**.
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.287 PWR-FAIL-A

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), cross-connect card, OC-N cards, or TCC2/TCC2P card.



Warning

The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment. Statement 207

Clear the PWR-FAIL-A Alarm

-
- Step 1** If a single card has reported the alarm, take the following actions depending on the reporting card:
- If the reporting card is an active traffic line port in a 1+1 or part of a path protection, ensure that an automatic protection switch (APS) traffic switch has occurred to move traffic to the protect port.



Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing”](#) section on page 2-260 for commonly used traffic-switching procedures.

- Step 2** If the alarm is reported against a TCC2/TCC2P card, complete the [“Reset an Active TCC2/TCC2P and Activate the Standby Card”](#) procedure on page 2-268.
- Step 3** If the alarm is reported against an OC-N card, complete the [“Reset a Traffic Card in CTC”](#) procedure on page 2-268.

- Step 4** If the alarm is reported against a cross-connect card, complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-268 for the cross-connect card. (The process is similar.)
- Step 5** If the alarm does not clear, complete the “[Remove and Reinsert \(Reseat\) Any Card](#)” procedure on page 2-270.
- Step 6** If the alarm does not clear, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the reporting card.
- Step 7** If the single card replacement does not clear the alarm, or if multiple cards report the alarm, verify the office power. Refer to the *Cisco ONS 15454 Procedure Guide* Chapter 1, “Install the Shelf and Backplane Cable,” for instructions to install power or refer to the *Cisco ONS 15454 Troubleshooting Guide* Chapter 1, “General Troubleshooting,” for power supply troubleshooting procedures.
- Step 8** If the alarm does not clear, reseat the power cable connection to the connector.
- Step 9** If the alarm does not clear, physically replace the power cable connection to the connector.
- Step 10** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.288 PWR-FAIL-B

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), cross-connect card, OC-N cards, or TCC2/TCC2P card.



Warning

The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment. Statement 207

Clear the PWR-FAIL-B Alarm

- Step 1** Complete the “[Clear the PWR-FAIL-A Alarm](#)” procedure on page 2-209.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.289 PWR-FAIL-RET-A

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the EIA, cross-connect card, OC-N cards, or TCC2/TCC2P card.

Clear the PWR-FAIL-RET-A Alarm:

-
- Step 1** Complete the [“Clear the PWR-FAIL-A Alarm” procedure on page 2-209](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.290 PWR-FAIL-RET-B

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the EIA, cross-connect card, OC-N cards, or TCC2/TCC2P card.

Clear the PWR-FAIL-RET-A Alarm

-
- Step 1** Complete the [“Clear the PWR-FAIL-A Alarm” procedure on page 2-209](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.291 RAI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

The Remote Alarm Indication condition signifies an end-to-end failure. The error condition is sent from one end of the SONET path to the other. RAI on a DS3XM-6 card indicates that the remote-node node is receiving a DS-3 AIS.

Clear the RAI Condition

-
- Step 1** Complete the [“Clear the AIS Condition” procedure on page 2-31](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.292 RCVR-MISS

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

A Facility Termination Equipment Receiver Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance usually occurs when a receive cable is missing from a DS-1 port, or a possible mismatch of backplane equipment occurs. For example, an SMB connector or a BNC connector might be misconnected to a DS-1 card.



Note

DS-1s are four-wire circuits and need a positive (tip) and negative (ring) connection for both transmit and receive.

Clear the RCVR-MISS Alarm

Step 1 Ensure that the device attached to the DS-1 port is operational.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the attachment is okay, verify that the cabling is securely connected.

Step 3 If the cabling is okay, verify that the pinouts are correct.

Step 4 If the pinouts are correct, replace the receive cable.

Step 5 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.293 RFI

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Remote Failure Indication condition is similar to the “[RFI-L](#)” condition on page 2-213 but it is raised against an MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card when it has the “[AIS](#)” condition on page 2-30. The MXP or TXP card only raise AIS (or remote failure indication [RFI]) when they are in line or section termination mode, that is, when the MXP or TXP cards in line termination mode or section termination mode has improperly terminated overhead bytes.

Clear the RFI Condition

Step 1 Complete the “[Delete a Circuit](#)” procedure on page 2-272 and then recreate the circuit.

- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.294 RFI-L

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: EC1, EC1-12, OCN

A RFI Line condition occurs when the ONS 15454 detects an RFI in OC-N card SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-L condition in the reporting node. RFI-L indicates that the condition is occurring at the line level.

Clear the RFI-L Condition

- Step 1** Log into the node at the remote-node node of the reporting ONS 15454.
- Step 2** Identify and clear any alarms, particularly the “[LOS \(OCN\)](#)” alarm on page 2-153.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.295 RFI-P

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

The RFI Path condition occurs when the ONS 15454 detects an RFI in the an STS-1 signal SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P condition in the reporting node. RFI-P occurs in the terminating node in that path segment.

Clear the RFI-P Condition

- Step 1** Verify that the ports are enabled and in service (IS-NR) on the reporting ONS 15454:
- a. Confirm that the LED is correctly illuminated on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 - b. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
 - c. Click the **Provisioning > Line** tabs.
 - d. Verify that the Admin State column lists the port as IS.
 - e. If the Admin State column lists the port as OOS,MT or OOS,DSLBD, click the column and choose **IS**. Click **Apply**.
- Step 2** To find the path and node failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.

- Step 3** Clear alarms in the node with the failure, especially the “UNEQ-P” alarm on page 2-249 or the “UNEQ-V” alarm on page 2-251.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.296 RFI-V

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: VT-TERM

An RFI VT Layer condition occurs when the ONS 15454 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-V condition in the reporting node. RFI-V indicates that an upstream failure has occurred at the VT layer.

Clear the RFI-V Condition

- Step 1** Verify that the connectors are securely fastened and connected to the correct slot. For more information, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 2** If connectors are correctly connected, verify that the DS-1 port is active and in service (IS-NR):
- Confirm that the LED is correctly illuminated on the physical card:
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 - To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
 - Click the **Provisioning > Line** tabs.
 - Verify that the Admin State column lists the port as IS.
 - If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.
- Step 3** If the ports are active and in service, use an optical test set to verify that the signal source does not have errors.
- For specific procedures to use the test set equipment, consult the manufacturer.
- Step 4** If the signal is valid, log into the node at the remote-node of the reporting ONS 15454.
- Step 5** Clear alarms in the remote node, especially the “UNEQ-P” alarm on page 2-249 or the “UNEQ-V” alarm on page 2-251.
- Step 6** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.297 RING-ID-MIS

- Default Severity: Major (MJ), Service Affecting (SA)
- Logical Objects: OCN, OSC-RING

The Ring ID Mismatch condition refers to the ring ID in APC. It occurs when a ring name does not match other detectable node ring names, and can cause problems with applications that require data exchange with APC. This alarm is similar to BLSR RING-MISMATCH, but rather than apply to ring protection, RING-ID-MIS applies to DWDM node discovery within the same network. For more information about APC, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the RING-ID-MIS Alarm

-
- Step 1** Complete the “[Clear the RING-MISMATCH Alarm](#)” procedure on page 2-215.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.298 RING-MISMATCH

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: OCN

A Procedural Error Mismatch Ring alarm occurs when the ring name of the ONS 15454 node that is reporting the alarm does not match the ring name of another node in the BLSR. Nodes connected in a BLSR must have identical ring names to function. This alarm can occur during BLSR provisioning.

RING-MISMATCH is somewhat similar to RING-ID-MIS, but it applies to BLSR protection discovery instead of DWDM node discovery.

Clear the RING-MISMATCH Alarm

-
- Step 1** In node view, click the **Provisioning > BLSR** tabs.
- Step 2** Note the name in the Ring Name field.
- Step 3** Log into the next ONS 15454 node in the BLSR.
- Step 4** Complete the “[Identify a BLSR Ring Name or Node ID Number](#)” procedure on page 2-259.
- Step 5** If the ring name matches the ring name in the reporting node, repeat **Step 4** for the next ONS 15454 in the BLSR.
- Step 6** Complete the “[Change a BLSR Ring Name](#)” procedure on page 2-259.
- Step 7** Verify that the ring map is correct.
- Step 8** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.299 RING-SW-EAST

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Ring Switch Is Active East Side condition occurs when a ring switch occurs at the east side of a BLSR using a Force Ring command. The condition clears when the switch is cleared.



Note

RING-SW-EAST is an informational condition and does not require troubleshooting.

2.8.300 RING-SW-WEST

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Ring Switch Is Active West Side condition occurs when a ring switch occurs at the west side of a BLSR using a Force Ring command. The condition clears when the switch is cleared.



Note

RING-SW-WEST is an informational condition and does not require troubleshooting.

2.8.301 RPRW

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: CE100T, ML100T, ML1000

The Resilient Packet Ring (RPR) Wrapped condition applies to CE100T-8 and ML-Series cards and occurs when the RPR protocol initiates a ring wrap due to a fiber cut, node failure, node restoration, new node insertion, or other traffic problem. It can also be raised if the POS port has an Admin down condition. (In this case, you will not see any SONET-level or TPTFAIL alarms.)

When the wrap occurs, traffic is redirected to the original destination by sending it in the opposite direction around the ring after a link state change or after receiving any SONET path-level alarms.



Note

ML-Series card POS interfaces normally send the “PDI-P” alarm on page 2-201 to the far end when the POS link goes down or when RPR wraps. ML-Series card POS interfaces do not send a PDI-P alarm to the far end when this alarm is detected, when the alarm is being sent to the far end, or when the only defects being detected are the “GFP-LFD” alarm on page 2-118, the “GFP-CSF” alarm on page 2-117, the VCAT “LOM” alarm on page 2-144, or the VCAT “SQM” alarm on page 2-230.



Note

For more information about CE-100T-8 and ML-Series Ethernet cards, refer to the <I_Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.

Clear the RPRW Condition

-
- Step 1** Look for and clear any service-affecting SONET path-level alarms on the affected circuit, such as the “LOP-P” alarm on page 2-145, “LOS-P (TRUNK)” alarm on page 2-163, “PLM-P” alarm on page 2-204, or the “TIM-P” alarm on page 2-243. Clearing this alarm can also clear RPRW.
- Step 2** If the condition does not clear, look for and clear any service alarms for the ML-Series card itself, such as the “CARLOSS (CE100T)” alarm on page 2-54, “CARLOSS (ML100T, ML1000)” alarm on page 2-62, “TPTFAIL (CE100T)” alarm on page 2-244, or the “TPTFAIL (ML100T, ML1000)” alarm on page 2-245.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.302 RUNCFG-SAVENEED

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Run Configuration Save Needed condition occurs when you change the running configuration file for ML1000-2 and ML100T-12 cards. It is a reminder that you must save the change to the startup configuration file for it to be permanent.

The condition clears after you save the running configuration to the startup configuration, such as by entering:

```
copy run start
```

at the privileged EXEC mode of the Cisco IOS CLI. If you do not save the change, the change is lost after the card reboots. If the command 'copy run start' is executed in configuration mode and not privileged EXEC mode, the running configuration will be saved, but the alarm will not clear.

**Note**

For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

2.8.303 SD (DS1, DS3)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A Signal Degrade (SD) condition for DS-1 or DS-3 occurs when the quality of an electrical signal has exceeded the BER signal degrade threshold. Signal degrade is defined by Telcordia as a soft failure condition. SD and also signal fail (SF) both monitor the incoming BER and are similar alarms, but SD is triggered at a lower bit error rate than SF.

The BER threshold is user provisionable and has a range for SD from 10^{-9} to 10^{-5} .

SD can be reported on electrical card ports that are In-Service and Normal (IS-NR); Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AIS); or Out-of-Service and Management, Maintenance (OOS-MA,MT) but not in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. The BER count increase associated with this alarm does not take an IS-NR port out of service, but if it occurs on an AINS port, the alarm prevents the port from going into service.

The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a faulty fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice. SD can also be caused by repeated XC10G cross-connect card switches that in turn can cause switching on the lines or paths.

**Warning**

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056

**Warning**

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

**Note**

Some levels of BER errors (such as 10^{-9}) take a long period to raise or clear, about 9,000 seconds, or 150 minutes. If the SD threshold is provisioned at 10^{-9} rate, the SD alarm needs at least one and a half hours to raise and then another period at least as long to clear.

**Note**

The recommended test set for use on all SONET ONS electrical cards is the Omniber 718.

Clear the SD (DS1, DS3) Condition

Step 1 Complete the [“Clear an OC-N Card Facility or Terminal Loopback Circuit” procedure on page 2-273.](#)

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”

Step 3 If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines.

For specific procedures to use the test set equipment, consult the manufacturer.

Step 4 If the optical power level is okay, verify that optical receive levels are within the acceptable range.

Step 5 If receive levels are okay, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

Step 6 If the condition does not clear, verify that single-mode fiber is used.

- Step 7** If the fiber is the correct type, verify that a single-mode laser is used at the remote-node node.
- Step 8** Clean the fiber connectors at both ends for a signal degrade according to site practice.
- Step 9** Verify that a single-mode laser is used at the remote node.
- Step 10** If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the “[2.11.4 Physical Card Reseating, Resetting, and Replacement](#)” section on page 2-269.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 11** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.304 SD (TRUNK)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

An SD condition on the trunk occurs when the quality of an optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card has BER on the incoming optical line that passes the signal degrade threshold. The alarm applies to the card ports and the trunk carrying optical or electrical signals to the card.

Signal degrade is defined by Telcordia as a soft failure condition. SD and SF both monitor the incoming BER and are similar alarms, but SD is triggered at a lower BER than SF. The BER threshold on the ONS 15454 is user provisionable and has a range for SD from 10^{-9} to 10^{-5} .

Clear the SD (TRUNK) Condition

- Step 1** Complete the “[Clear the SD \(DS1, DS3\) Condition](#)” procedure on page 2-218.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.305 SD-L

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EC1, EC1-12, OCN

An SD Line condition is similar to the “SD (DS1, DS3)” condition on page 2-217. It applies to the line level of the SONET signal and travels on the B2 byte of the SONET overhead.

An SD-L on an Ethernet or OC-N card does not cause a protection switch. If the alarm is reported on a card that has also undergone a protection switch, the SD BER count continues to accumulate. The alarm is superseded by higher-priority alarms such as 2.8.176 LOF (EC1), 2.8.177 LOF (OCN), 2.8.188 LOS (EC1, EC1-12), and 2.8.193 LOS (OCN), page 2-153.

Clear the SD-L Condition

-
- Step 1** Complete the “Clear the SD (DS1, DS3) Condition” procedure on page 2-218.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.306 SD-P

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM, VT-TERM

An SD Path condition is similar to the “SD (DS1, DS3)” condition on page 2-217, but it applies to the path (STS) layer of the SONET overhead. A path or STS-level SD alarm travels on the B3 byte of the SONET overhead.

For path protection protected circuits, the BER threshold is user provisionable and has a range for SD from 10^{-9} to 10^{-5} . For BLSR 1+1 and unprotected circuits, the BER threshold value is not user provisionable and the error rate is hard-coded to 10^{-6} .

On path protection, an SD-P condition causes a switch from the working card to the protect card at the path (STS) level. On BLSR, 1+1, and on unprotected circuits, an SD-P condition does not cause switching.

The BER increase that causes the alarm is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Signal degrade and signal fail both monitor the incoming BER and are similar alarms, but SD is triggered at a lower BER than SF. SD causes the card to switch from working to protect. The SD alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the SD-P Condition

-
- Step 1** Complete the “Clear the SD (DS1, DS3) Condition” procedure on page 2-218.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.307 SD-V

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: VT-MON

An SD-V condition is similar to the “SD (DS1, DS3)” condition on page 2-217, but it applies to the VT layer of the SONET overhead.

For path protection protected circuits, the BER threshold is user provisionable and has a range for SD from 10^{-9} to 10^{-5} . For BLSR 1+1 and unprotected circuits, the BER threshold value is not user provisionable and the error rate is hard-coded to 10^{-6} .

On path protection configurations, an SD-V condition does not cause a switch from the working card to the protect card at the path (STS) level. On BLSR, 1+1, and on unprotected circuits, an SD-V condition does not cause switching.

The BER increase that causes the alarm is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Signal degrade and signal fail both monitor the incoming BER and are similar alarms, but SD is triggered at a lower BER than SF. SD causes the card to switch from working to protect. The SD alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the SD-V Condition

-
- Step 1** Complete the “Clear the SD (DS1, DS3) Condition” procedure on page 2-218.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.308 SF (DS1, DS3)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A Signal Fail (SF) condition occurs when the quality of the signal has exceeded the BER signal failure threshold. Signal failure is defined by Telcordia as a “hard failure” condition. The SD and SF conditions both monitor the incoming BER error rate and are similar conditions, but SF is triggered at a higher BER than SD.

The BER threshold is user provisionable and has a range for SF from 10^{-5} to 10^{-3} .



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

Clear the SF (DS1, DS3) Condition

Step 1 Complete the “[Clear the SD \(DS1, DS3\) Condition](#)” procedure on page 2-218.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.309 SF (TRUNK)

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

An SF condition for the trunk occurs when the quality of an optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card has BER on the incoming optical line that passes the signal fail threshold. The alarm applies to the card ports and the trunk carrying optical or electrical signals to the card.

Signal fail is defined by Telcordia as a hard failure condition. SF monitors the incoming BER and is triggered when the BER surpasses the default range.



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

Clear the SF (TRUNK) Condition

Step 1 Complete the “[Clear the SD \(DS1, DS3\) Condition](#)” procedure on page 2-218.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.310 SF-L

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EC1, EC1-12, OCN

An SF Line condition is similar to the “[SF \(DS1, DS3\) condition on page 2-221](#)”, but it applies to the line layer B2 overhead byte of the SONET signal. It can trigger a protection switch.

The SF-L condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The alarm is superseded by higher-priority alarms such as [2.8.176 LOF \(EC1\)](#), [2.8.188 LOS \(EC1, EC1-12\)](#), and [2.8.193 LOS \(OCN\)](#), [page 2-153](#).

Clear the SF-L Condition

-
- Step 1** Complete the “[Clear the SD \(DS1, DS3\) Condition](#)” [procedure on page 2-218](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.311 SF-P

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM, VT-TERM

An SF Path condition is similar to an “[SF \(DS1, DS3\) condition on page 2-221](#)”, but it applies to the path (STS) layer B3 byte of the SONET overhead. It can trigger a protection switch.

The SF-P condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Clear the SF-P Condition

-
- Step 1** Complete the “[Clear the SD \(DS1, DS3\) Condition](#)” [procedure on page 2-218](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.312 SF-V

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: VT-MON

An SF-V condition is similar to the “[SF \(DS1, DS3\) condition on page 2-221](#)”, but it applies to the VT layer of the SONET overhead.

Clear the SF-V Condition

-
- Step 1** Complete the “[Clear the SD \(DS1, DS3\) Condition](#)” procedure on page 2-218.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.313 SFTWDOWN

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: EQPT

A Software Download in Progress alarm occurs when the TCC2/TCC2P is downloading or transferring software.

If the active and standby TCC2/TCC2Ps have the same versions of software, it takes approximately three minutes for software to be updated on a standby TCC2/TCC2P.

If the active and standby TCC2/TCC2Ps have different software versions, the transfer can take up to 30 minutes. Software transfers occur when different software versions exist on the two cards. After the transfer completes, the active TCC2/TCC2P reboots and goes into standby mode after approximately three minutes.

No action is necessary. Wait for the transfer or the software download to complete. If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).



Note

SFTWDOWN is an informational alarm.

2.8.314 SH-INS-LOSS-VAR-DEG-HIGH

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OTS

The Switch Insertion Loss Variation Degrade High alarm occurs as the OSC-CSM card optical switch ages and slowly increases its insertion loss. This alarm indicates that the insertion loss has crossed the high degrade threshold. The card must be replaced eventually.

2.8.314.1 Clear the SH-INS-LOSS-VAR-DEG-HIGH Alarm

-
- Step 1** For the alarmed card, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 as appropriate.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.315 SH-INS-LOSS-VAR-DEG-LOW

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OTS

The Switch Insertion Loss Variation Degrade Low alarm occurs as the OSC-CSM card optical switch ages and slowly decreases its insertion loss. This alarm indicates that the insertion loss has crossed the low degrade threshold. The card must eventually be replaced.

2.8.315.1 Clear the SH-INS-LOSS-VAR-DEG-LOW Alarm

-
- Step 1** For the alarmed card, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 as appropriate.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.316 SHUTTER-OPEN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OTS

The SHUTTER-OPEN condition occurs if an OSC-CSM card laser shutter remains open after the [2.8.194 LOS \(OTS\)](#) alarm is detected. A laser shutter remains open if an optical safety issue is present and closes when the OSC-CSM card LINE-RX port receives OSC power for three consecutive seconds.

Clear the SHUTTER-OPEN Condition


-
- Step 1** Complete the “[Clear the LOS \(OTS\) Alarm](#)” procedure on page 2-155.
- Step 2** If the SHUTTER-OPEN condition still does not clear, it indicates that the unit shutter is not working properly. Complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.317 SIGLOSS

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: FC, FCMR, GE, ISC, TRUNK

The Signal Loss on Data Interface alarm is raised on FC_MR-4 card receive client ports when there is an LOS. It can be cleared by a terminal loopback state on the FC_MR-4 port. SIGLOSS demotes the SYNCLOSS alarm.

Clear the SIGLOSS Alarm

-
- Step 1** Ensure that the Fibre Channel data port connection at the local card port of the SONET link is operational.
- Step 2** Verify fiber continuity to the port.
-  **Note** To verify fiber continuity, follow site practices.
-
- Step 3** Check the physical port LED on the Fibre Channel card. The port LED looks clear (that is, not lit green) if the link is not connected.
- Step 4** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.318 SNTP-HOST

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: NE

The Simple Network Timing Protocol (SNTP) Host Failure alarm indicates that an ONS 15454 serving as an IP proxy for the other ONS 15454s in the ring is not forwarding SNTP information to the other nodes in the network. The forwarding failure can result from two causes: either the IP network attached to the ONS 15454 proxy node is experiencing problems, or the ONS 15454 proxy node itself is not functioning properly.

Clear the SNTP-HOST Alarm

-
- Step 1** Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet.
- Step 2** If the ping fails, contact the network administrator who manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems which could affect the SNTP server/router connecting to the proxy ONS 15454 system.
- Step 3** If no network problems exist, ensure that the ONS system proxy is provisioned correctly:
- In node view for the ONS 15454 serving as the proxy, click the **Provisioning > General** tabs.
 - Ensure that the Use NTP/SNTP Server check box is checked.
 - If the Use NTP/SNTP Server check box is not checked, click it.
 - Ensure that the Use NTP/SNTP Server field contains a valid IP address for the server.
- Step 4** If proxy is correctly provisioned, refer to the *<I_Ital>Cisco ONS 15454 Reference Manual* for more information on SNTP Host.
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.319 SPAN-SW-EAST

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Span Switch Is Active East Side condition occurs when a span switch occurs at the east side of a four-fiber BLSR span using a Force Span command. The condition clears when the switch is cleared.



Note

SPAN-SW-EAST is an informational condition and does not require troubleshooting.

2.8.320 SPAN-SW-WEST

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Span Switch Is Active West Side condition occurs when a span switch occurs at the west side of a four-fiber BLSR span using a Force Span command. The condition clears when the switch is cleared.



Note

SPAN-SW-WEST is an informational condition and does not require troubleshooting.

2.8.321 SQUELCH

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: OCN

The Ring Squelching Traffic condition occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance Force Ring commands. The isolation or failure of the node disables circuits that originate or terminate on the failed node. SQUELCH conditions appear on one or both of the nodes on either side of the isolated or failed node. The [“AIS-P” condition on page 2-31](#) also appears on all nodes in the ring except the isolated node.



Warning

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293.



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

Clear the SQUELCH Condition

- Step 1** Determine the isolated node:
- In node view, click **View > Go to Network View**.
 - The grayed out node with red spans is the isolated node.

- Step 2** Verify fiber continuity to the ports on the isolated node.



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.



Note

To verify fiber continuity, follow site practices.

- Step 3** If fiber continuity is okay, verify that the proper ports are in service:
- Confirm that the LED is correctly illuminated on the physical card.
A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
 - To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.
 - Click the **Provisioning > Line** tabs.
 - Verify that the Admin State column lists the port as IS.
 - If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.
- Step 4** If the correct ports are in service, use an optical test set to verify that a valid signal exists on the line.
For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.
- Step 5** If the signal is valid, verify that the power level of the optical signal is within the optical card receiver specifications. Refer to the *<I_Ital>Cisco ONS 15454 Reference Manual* for card specifications.
- Step 6** If the receiver levels are okay, ensure that the optical transmit and receive fibers are connected properly.
- Step 7** If the connectors are okay, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the OC-N card.



Caution

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.



Note

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 8** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.322 SQUELCHED

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, ESCON, FC, GE, ISC, OCN, TRUNK

The Client Signal Squelched condition is raised by a TXP_MR_10G, TXP_MR_10E, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, MXP_2.5G_10E, MXP_MR_2.5G, or MXPP_MR_2.6G card.

The condition can be raised in the following situations:

- An MXP or TXP client facility detects that an upstream Rx facility has experienced a loss of signal (such as an Ethernet CARLOSS, DWDM SIGLOSS, or optical LOS). In response, the facility's Tx is turned off (SQUELCHED). The upstream Rx facilities are the trunk Rx on the same card as the client, as well as the client Rx on the card at the other end of the trunk span.
- The client will squelch if the upstream trunk Rx (on the same card) experiences a SIGLOSS, Ethernet CARLOSS, LOS, or LOS (TRUNK) alarm. In some transparent modes, the client is squelched if the trunk detects an AIS condition or a TIM alarm.
- The client will squelch if the upstream client Rx (on the card at the other end of the DWDM span) experiences CARLOSS, SIGLOSS, or LOS.

In an example situation, an upstream MXP_2.5G_10G client port Rx experiences a "loss of light," and this port raises CARLOSS, SIGLOSS, or LOS (determined by the payload type) locally. The port also sends client signal fail (GFP-CSF) to its downstream card. The downstream card raises a GFP-CSF alarm, turns off the client Tx laser, and raises the SQUELCHED condition.

The local client raises SQUELCHED if it also raises one of the following alarms, all of which are signalled by the upstream node:

- ["GFP-CSF" alarm on page 2-117](#) for the client
- ["GFP-LFD" alarm on page 2-118](#) for the client
- ["GFP-NO-BUFFERS" alarm on page 2-119](#) for the client
- ["GFP-DE-MISMATCH" alarm on page 2-117](#) for the client
- ["GFP-EX-MISMATCH" alarm on page 2-118](#) for the client
- ["ODUK-1-AIS-PM" alarm on page 2-187](#) for the client
- ["ODUK-2-AIS-PM" alarm on page 2-187](#) for the client
- ["ODUK-3-AIS-PM" alarm on page 2-188](#) for the client
- ["ODUK-4-AIS-PM" alarm on page 2-188](#) for the client

On the MXP_MR_10G, the local client raises SQUELCHED if the upstream client detects one of the following alarms. Note that no corresponding local alarm is raised to indicate which of these conditions is present upstream.

- LOS for the clients including ["LOS \(2R\)" alarm on page 2-147](#), ["LOS \(ESCON\)" alarm on page 2-151](#), and ["LOS \(ISC\)" alarm on page 2-152](#)
- CARLOSS for the clients including ["CARLOSS \(FC\)" alarm on page 2-58](#), ["CARLOSS \(GE\)" alarm on page 2-61](#), and ["CARLOSS \(ISC\)" alarm on page 2-61](#)

The local client raises SQUELCHED if the local trunk raises one of the following alarms:

- ["OTUK-LOF" alarm on page 2-199](#) for the trunk
- ["OTUK-AIS" alarm on page 2-197](#) for the trunk
- ["LOS \(TRUNK\)" alarm on page 2-156](#)

- “OTUK-TIM” alarm on page 2-200 squelching enabled, for the trunk
- “ODUK-AIS-PM” alarm on page 2-188 for the trunk
- “ODUK-LCK-PM” alarm on page 2-189 for the trunk
- “ODUK-TIM-PM” alarm on page 2-191 with squelching enabled, for the trunk
- “TIM” alarm on page 2-242 with squelching enabled, for OC-N
- “LOF (OCN)” alarm on page 2-143
- “LOS (OCN)” alarm on page 2-153
- “CARLOSS (TRUNK)” alarm on page 2-63
- “WVL-MISMATCH” alarm on page 2-256 for the client or trunk

When troubleshooting the SQUELCHED condition locally, look for failures progressing upstream in the following order. (If you are troubleshooting this alarm remotely, reverse the order of progress.)

- Local client alarms, as above
- Local trunk alarms, as above
- Remote (upstream) client Rx alarms, as above

**Note**

Note: If you see a SQUELCHED condition on the trunk, this can only be caused by a transponder (TXP) card.

Clear the SQUELCHED Condition

-
- Step 1** If the object is reported against any object besides ESCON, determine whether the remote node and local node reports and LOF or the LOS alarm (for the client trunk, as listed above). If it does, turn to the relevant section in this chapter and complete the troubleshooting procedure.
- Step 2** If no LOF or LOS is reported, determine whether any other listed remote node or local node conditions as listed above has occurred. If so, turn to the relevant section of this chapter and complete the troubleshooting procedure.
- Step 3** If none of these alarms is reported, determine whether the local port reporting the SQUELCHED condition is in loopback. (You will see LPBKFACILITY OR LPBKTERMINAL in the condition window for this port.) If it is in loopback, complete the following steps:
- Double-click the client card to display the card view.
 - Click the **Maintenance > Loopback > Port** tabs.
 - If the port Admin State column says OOS,MT or OOS,DSBLD, click the cell to highlight it and choose **IS** from the drop-down list. Changing the state to IS also clears any loopback provisioned on the port.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.323 SQM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: STSTRM, VT-TERM

The Sequence Mismatch alarm is a virtual concatenated (VCAT) member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when the expected sequence numbers of VCAT members do not match the received sequence numbers.

Clear the SQM Alarm

-
- Step 1** For the errored circuit, complete the “Delete a Circuit” procedure on page 2-272.
- Step 2** Recreate the circuit using the procedure in the “Manage Circuits” chapter of the *Cisco ONS 15454 Procedure Guide* Chapter 6, “Create Circuits and Tunnels.”
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.324 SSM-DUS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, OCN, TRUNK

The Synchronization Status (SSM) Message Quality Changed to Do Not Use (DUS) condition occurs when the synchronization status message (SSM) quality level degrades to DUS or is manually changed to DUS.

The signal is often manually changed to DUS to prevent timing loops from occurring. Sending a DUS prevents the timing from being reused in a loop. The DUS signal can also be sent for line maintenance testing.

**Note**

SSM-DUS is an informational condition and does not require troubleshooting.

2.8.325 SSM-FAIL

- Single Failure Default Severity: Minor (MN), Non-Service Affecting (NSA); Double Failure Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: BITS, DS1, OCN, TRUNK

The SSM Failed alarm occurs when the synchronization status messaging received by the ONS 15454 fails. The problem is external to ONS 15454. The ONS 15454 is set up to receive SSM, but the timing source is not delivering valid SSM messages.

Clear the SSM-FAIL Alarm

-
- Step 1** Verify that SSM is enabled on the external timing source.
- Step 2** If timing is enabled, use an optical test set to determine that the external timing source is delivering SSM. For specific procedures to use the test set equipment, consult the manufacturer.

- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.326 SSM-LNC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The SSM Local Node Clock (LNC) Traceable condition occurs when the SSM (S1) byte of the SONET overhead multiplexing section has been changed to signify that the line or BITS timing source is the LNC.



Note

SSM-LNC is an informational condition and does not require troubleshooting.

2.8.327 SSM-OFF

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, OCN, TRUNK

The SSM Off condition applies to references used for timing the node. It occurs when the SSM for the reference has been turned off. The ONS system is set up to receive SSM, but the timing source is not delivering SSM messages.

Clear the SSM-OFF Condition

- Step 1** Complete the [“Clear the SSM-FAIL Alarm” procedure on page 2-231](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.328 SSM-PRC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The SSM Primary Reference Clock (PRC) Traceable condition occurs when the SONET transmission level is changed to PRC.



Note

SSM-PRC is an informational condition and does not require troubleshooting.

2.8.329 SSM-PRS

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Primary Reference Source (PRS) Traceable condition occurs when the SSM transmission level is changed to Stratum 1 Traceable.



Note

SSM-PRS is an informational condition and does not require troubleshooting.

2.8.330 SSM-RES

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Reserved (RES) For Network Synchronization Use condition occurs when the synchronization message quality level is changed to RES.



Note

SSM-RES is an informational condition and does not require troubleshooting.

2.8.331 SSM-SDN-TN

The SSM-SDN-TN condition is not used in this platform in this release. It is reserved for future development.

2.8.332 SSM-SETS

The SSM-SETS condition is not used in this platform in this release. It is reserved for future development.

2.8.333 SSM-SMC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM SONET Minimum Clock (SMC) Traceable condition occurs when the synchronization message quality level changes to SMC. The login node does not use the clock because the node cannot use any reference beneath its internal level, which is ST3.



Note

SSM-SMC is an informational condition and does not require troubleshooting.

2.8.334 SSM-ST2

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Stratum 2 (ST2) Traceable condition occurs when the synchronization message quality level is changed to ST2.



Note

SSM-ST2 is an informational condition and does not require troubleshooting.

2.8.335 SSM-ST3

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Stratum 3 (ST3) Traceable condition occurs when the synchronization message quality level is changed to ST3.



Note

SSM-ST3 is an informational condition and does not require troubleshooting.

2.8.336 SSM-ST3E

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Stratum 3E (ST3E) Traceable condition indicates that the synchronization message quality level is changed to ST3E from a lower level of synchronization. SSM-ST3E is a Generation 2 SSM and is used for Generation 1.



Note

SSM-ST3E is an informational condition and does not require troubleshooting.

2.8.337 SSM-ST4

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Stratum 4 (ST4) Traceable condition occurs when the synchronization message quality level is lowered to ST4. The message quality is not used because it is below ST3.



Note

SSM-ST4 is an informational condition and does not require troubleshooting.

2.8.338 SSM-STU

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Synchronization Traceability Unknown (STU) condition occurs when the reporting node is timed to a reference that does not support SSM, but the ONS 15454 has SSM support enabled. STU can also occur if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15454.

Clear the SSM-STU Condition

-
- Step 1** In node view, click the **Provisioning > Timing** tabs.
- Step 2** Complete one of the following depending upon the status of the Sync Messaging Enabled check box:
- If the **Sync Messaging Enabled** check box for the BITS source is checked, uncheck the box.
 - If the **Sync Messaging Enabled** check box for the BITS source is not checked, check the box.
- Step 3** Click **Apply**.
- Step 4** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.339 SSM-TNC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, DS1, NE-SREF, OCN, TRUNK

The SSM Transit Node Clock (TNC) Traceable condition occurs when the synchronization message quality level is changed to TNC.



Note

SSM-TNC is an informational condition and does not require troubleshooting.

2.8.340 SWMTXMOD

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Object: EQPT

The Switching Matrix Module Failure alarm occurs on cross-connect cards and traffic cards. If the alarm reports against a traffic card, it occurs when the logic component on the cross-connect card is out of frame (OOF) with the logic component on the reporting traffic card. All traffic on the reporting traffic card is lost.

If the alarm reports against a cross-connect card, it occurs when a logic component internal to the reporting cross-connect card is OOF with a second logic component on the same cross-connect card. One or more traffic cards could lose traffic as a result of the cross-connect frame failure.

In R5.0, the alarm initiates an autonomous switch in 1+1, 1:1, 1:N, path protection, and BLSR protection schemes if it is raised on the following I/O cards: DS-1, DS3-E, DS3-CR, OC-12, OC-48 IR, and OC-48 ELR. The switching time is greater than 60 milliseconds and typically lasts approximately 500 milliseconds.

If the alarm is raised against active XCVT card, an autonomous switch to the standby XCVT occurs under the following circumstances:

- The standby XCVT does not have an SWMTXMOD alarm active.
- No lockout condition is present on the XCVT card.

If the standby XCVT does has an active SWMTXMOD alarm, the cross-connect switch request from CTC or TL1 is denied.

Clear the SWMTXMOD Alarm

-
- Step 1** If the card reporting the alarm is the standby cross-connect card, complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for the card. For the LED behavior, see the [“2.10.2 Typical Traffic Card LED Activity During Reset” section on page 2-258](#).
- Step 2** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 3** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-270](#) for the standby cross-connect card.
- Step 4** If the card reporting the alarm is the active cross-connect card, complete the [“Side Switch the Active and Standby XC10G Cross-Connect Cards” procedure on page 2-269](#).



Note After the active cross-connect card goes into standby mode, the original standby slot becomes active. The former standby card ACT/SBY LED becomes green.

- Step 5** If the card reporting the alarm is not the active cross-connect card or if you completed the side switch in [Step 4](#), complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for the reporting card. For the LED behavior, see the [“2.10.2 Typical Traffic Card LED Activity During Reset” section on page 2-258](#).
- Step 6** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 7** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-270](#) for the standby cross-connect card.
- Step 8** If the card reporting the alarm is a traffic card, complete the [“Side Switch the Active and Standby XC10G Cross-Connect Cards” procedure on page 2-269](#).
- Step 9** If the alarm does not clear, complete the [“Reset a Traffic Card in CTC” procedure on page 2-268](#) for the reporting card. For the LED behavior, see the [“2.10.2 Typical Traffic Card LED Activity During Reset” section on page 2-258](#).
- Step 10** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- Step 11** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) Any Card” procedure on page 2-270](#) for the traffic line card.

- Step 12** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.341 SWTOPRI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Primary Reference condition occurs when the ONS 15454 switches to the primary timing source (reference 1). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.



Note

SWTOPRI is an informational condition and does not require troubleshooting.

2.8.342 SWTOSEC

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Secondary Reference condition occurs when the ONS 15454 has switched to the secondary timing source (reference 2). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Clear the SWTOSEC Condition

- Step 1** To clear the condition, clear alarms related to failures of the primary source, such as the “[SYNCPRI](#)” alarm on page 2-239.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.343 SWTOTHIRD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Third Reference condition occurs when the ONS 15454 has switched to the third timing source (reference 3). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Clear the SWTOTHIRD Condition

-
- Step 1** To clear the condition, clear alarms related to failures of the primary source, such as the “[SYNCPRI](#)” alarm on page 2-239 or the “[SYNCSEC](#)” alarm on page 2-240.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.344 SYNC-FREQ

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, OCN, TRUNK

The Synchronization Reference Frequency Out of Bounds condition is reported against any reference that is out of the bounds for valid references. The login node fails the reference and chooses another internal or external reference to use.

Clear the SYNC-FREQ Condition

-
- Step 1** Use an optical test set to verify the timing frequency of the line or BITS timing source and ensure that it falls within the proper frequency.
- For specific procedures to use the test set equipment, consult the manufacturer.
- For BITS, the proper timing frequency range is approximately –15 PPM to 15 PPM. For optical line timing, the proper frequency range is approximately –16 PPM to 16 PPM.
- Step 2** If the reference source frequency is not outside of bounds, complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the TCC2/TCC2P.



Note When you replace a card with an identical type of card, you do not need to make any changes to the database.



Note It takes up to 30 minutes for the TCC2/TCC2P to transfer the system software to the newly installed TCC2/TCC2P. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the active TCC2/TCC2P reboots and goes into standby mode after approximately three minutes.

- Step 3** If the SYNC-FREQ condition continues to report after replacing the TCC2/TCC2P card, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.345 SYNCLOSS

- Default Severity: Major (MJ), Service-Affecting (SA)

- Logical Objects: FC, FCMR, GE, ISC, TRUNK

The Loss of Synchronization on Data Interface alarm is raised on FC_MR-4 cards when there is a loss of signal synchronization on the client port. This alarm can raise on the FC_MR-4 local port when the port is put into terminal loopback state (LPBKTERMINAL). This alarm is demoted by the SIGLOSS alarm.

Clear the SYNCLOSS Alarm

-
- Step 1** Ensure that the fibre channel data port connection at the near-end card port of the SONET link is operational.
- Step 2** Verify fiber continuity to the port. To do this follow site practices.
- Step 3** View the FC_MR-4 physical port LED to determine whether the alarm has cleared.
- If the port LED to determine the card's status:
- If the is green, the alarm has cleared.
 - If the port LED is clear (that is, not illuminated green), the link is not connected and the alarm has not cleared.
 - If the LED is red, this indicates that the fiber is pulled.
- Step 4** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.8.346 SYNCPRI

- Default Severity: Minor (MN), Non-Service Affecting (NSA) for EXT-SREF; Major (MJ), Service-Affecting (SA) for NE-SREF
- Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Primary Reference alarm occurs when the ONS 15454 loses the primary timing source (reference 1). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the ONS 15454 should switch to its secondary timing source (reference 2). Switching to the secondary timing source also triggers the “[SWTOSEC](#)” alarm on [page 2-237](#).

Clear the SYNCPRI Alarm

-
- Step 1** In node view, click the **Provisioning > Timing** tabs.
- Step 2** Verify the current configuration for the REF-1 of the NE Reference.
- Step 3** If the primary timing reference is a BITS input, complete the “[Clear the LOS \(BITS\) Alarm](#)” procedure on [page 2-148](#).
- Step 4** If the primary reference clock is an incoming port on the ONS 15454, complete the “[Clear the LOS \(OCN\) Alarm](#)” procedure on [page 2-153](#).

- Step 5** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.347 SYNCSEC

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Secondary Reference alarm occurs when the ONS 15454 loses the secondary timing source (reference 2). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCSEC occurs, the ONS 15454 should switch to the third timing source (reference 3) to obtain valid timing for the ONS 15454. Switching to the third timing source also triggers the “[SWTOTHIRD](#)” alarm on [page 2-237](#).

Clear the SYNCSEC Alarm

- Step 1** In node view, click the **Provisioning > Timing** tabs.
- Step 2** Verify the current configuration of the REF-2 for the NE Reference.
- Step 3** If the second reference is a BITS input, complete the “[Clear the LOS \(BITS\) Alarm](#)” procedure on [page 2-148](#).
- Step 4** Verify that the BITS clock is operating properly.
- Step 5** If the secondary timing source is an incoming port on the ONS 15454, complete the “[Clear the LOS \(OCN\) Alarm](#)” procedure on [page 2-153](#).
- Step 6** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.348 SYNCTHIRD

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Third Reference alarm occurs when the ONS 15454 loses the third timing source (reference 3). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCTHIRD occurs and the ONS 15454 uses an internal reference for source three, the TCC2/TCC2P card might have failed. The ONS 15454 often reports either the “[FRNGSYNC](#)” condition on [page 2-112](#) or the “[HLDOVRSYNC](#)” condition on [page 2-125](#) after a SYNCTHIRD alarm.

Clear the SYNCTHIRD Alarm

- Step 1** In node view, click the **Provisioning > Timing** tabs.

- Step 2** Verify that the current configuration of the REF-3 for the NE Reference. For more information about references, refer to the *<I_Ital>Cisco ONS 15454 Reference Manual Chapter 9, “Security and Timing.”*
- Step 3** If the third timing source is a BITS input, complete the “[Clear the LOS \(BITS\) Alarm](#)” procedure on page 2-148.
- Step 4** If the third timing source is an incoming port on the ONS 15454, complete the “[Clear the LOS \(OCN\) Alarm](#)” procedure on page 2-153.

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 5** If the third timing source uses the internal ONS 15454 timing, complete the “[Reset an Active TCC2/TCC2P and Activate the Standby Card](#)” procedure on page 2-268.
- Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
- Step 6** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseal the card, complete “[Remove and Reinsert \(Reseat\) the Standby TCC2/TCC2P Card](#)” procedure on page 2-270. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the “[Physically Replace a Traffic Card](#)” procedure on page 2-271.

2.8.349 SYSBOOT

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: NE

The System Reboot alarm indicates that new software is booting on the TCC2/TCC2P card. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes.

If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Note**

SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

2.8.350 TEMP-MISM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: NE

Temperature Reading Mismatch Between Control Cards is raised when the temperature readings on the two TCC2/TCC2Ps are out of range of each other by more than some predefined difference (such as 5 degrees C). A message containing power monitoring and temperature information is exchanged between the two TCC2/TCC2Ps, allowing the values to be compared. The temperature of each TCC2/TCC2P is read from a system variable.

This condition can be caused by a clogged fan filter or by fan tray stoppage.

Clear the TEMP-MISM Condition

-
- Step 1** Complete the [“Inspect, Clean, and Replace the Reusable Air Filter”](#) procedure on page 2-275.
 - Step 2** If the condition does not clear, complete the [“Remove and Reinsert a Fan-Tray Assembly”](#) procedure on page 2-277.
 - Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.351 TIM

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: OCN, TRUNK

The Section TIM alarm occurs when the expected J0 section trace string does not match the received section trace string.

If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Follow the procedure below to clear either instance.

TIM occurs on a port that has previously been operating without alarms if someone switches optical fibers that connect the ports. TIM is usually accompanied by other alarms, such as the [“LOS \(OCN\)”](#) alarm on page 2-153 or the [“UNEQ-P”](#) alarm on page 2-249. If these alarms accompany TIM, reattach or replace the original cables/fibers to clear the alarms. If a Transmit or Expected String was changed, restore the original string.

Clear the TIM Alarm

-
- Step 1** Log into the circuit source node and click the **Circuits** tab.
 - Step 2** Select the circuit reporting the condition, then click **Edit**.
 - Step 3** In the Edit Circuit window, check the **Show Detailed Map** box.
 - Step 4** On the detailed circuit map, right-click the source circuit port and choose **Edit J0 Path Trace (port)** from the shortcut menu.
 - Step 5** Compare the Current Transmit String and the Current Expected String entries in the Edit J0 Path Trace dialog box.
 - Step 6** If the strings differ, correct the Transmit or Expected strings and click **Apply**.
 - Step 7** Click **Close**.
 - Step 8** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem if necessary.
-

2.8.352 TIM-MON

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: OCN, TRUNK

The TIM Section Monitor Trace Identifier Mismatch alarm is similar to the “TIM-P” alarm on [page 2-243](#), but it applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when they are configured in transparent mode. (In transparent termination mode, all SONET overhead bytes are passed through from client ports to the trunk ports or vice versa.)

Clear the TIM-MON Alarm

-
- Step 1** Complete the “[Clear the TIM-P Alarm](#)” procedure on [page 2-243](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.353 TIM-P

- Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM; Default Severity: Minor (MN), Non-Service Affecting (NSA) for STSMON
- Logical Objects: STSMON, STSTRM

The TIM Path alarm occurs when the expected path trace string does not match the received path trace string. Path Trace Mode must be set to Manual or Auto for the TIM-P alarm to occur.

In manual mode at the Path Trace window, the user types the expected string into the Current Expected String field for the receiving port. The string must match the string typed into the Transmit String field for the sending port. If these fields do not match, the login node raises the TIM-P alarm. In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Complete the following procedure to clear either instance.

TIM-P also occurs on a port that has previously been operating without alarms if someone switches or removes the DS-3 cables or optical fibers that connect the ports. TIM-P is usually accompanied by other alarms, such as the “LOS (OCN)” alarm on [page 2-153](#), the “UNEQ-P” alarm on [page 2-249](#), or the “PLM-P” alarm on [page 2-204](#). If these alarms accompany TIM-P, reattach or replace the original cables/fibers to clear the alarms.

Clear the TIM-P Alarm

-
- Step 1** Complete the “[Clear the TIM Alarm](#)” procedure on [page 2-242](#).
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447). If the alarm applies to the STSTRM object, it is service-affecting.
-

2.8.354 TIM-V

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: VT-TERM

The VT Path Trace Identifier Mismatch alarm is raised on VT terminations when the the J2 path trace is enabled and is mismatched with the expected trace string.

Clear the TIM-V Alarm

-
- Step 1** Complete the “[Clear the TIM Alarm](#)” procedure on page 2-242.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.8.355 TPTFAIL (CE100T)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: CE100T

The Transport (TPT) Layer Failure alarm for the CE-100T-8 card indicates a break in the end-to-end Ethernet link integrity feature of the ONS 15454 CE-100T-8 card. TPTFAIL indicates a remote-node condition and not a problem with the port reporting TPTFAIL.

Clear the TPTFAIL (CE100T) Alarm

-
- Step 1** Complete the “[Clear the TPTFAIL \(G1000\) Alarm](#)” procedure on page 2-245.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.8.356 TPTFAIL (FCMR)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: FCMR

The Transport Fail alarm is raised against a local Fibre Channel (FC) port on an FC_MR-4 card when the port receives another SONET error such as AIS-P, LOP-P, UNEQ-P, PLM-P, TIM-P, LOM (for VCAT only), or SQM (for VCAT only).

This TPTFAIL can be raised against Fibre Channel cards if the remote FC card port is down from SIGLOSS or SYNCLOSS. In that case, the remote FC card port sends a PDI-P error code in the SONET C2 byte and signals the local FC port transmitter to turn off (thus causing the local FC port to raise the TPTFAIL alarm). A TPTFAIL can also be raised when a remote-node Rx fiber is pulled. This alarm can be demoted when a facility loopback is placed on the FC_MR-4 port.

Clear the TPTFAIL (FCMR) Alarm

-
- Step 1** Find and clear any path alarms applying to the port. Refer to the correct section of this chapter for trouble clearing instructions. Clearing the path alarm also clears the TPTFAIL.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.357 TPTFAIL (G1000)

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: G1000

The Transport Layer Failure alarm for the G-Series Ethernet cards indicates a break in the end-to-end Ethernet link integrity feature of the ONS 15454 G1000-4 cards. TPTFAIL indicates a remote-node condition and not a problem with the port reporting TPTFAIL.

The TPTFAIL alarm indicates a problem on either the SONET path or the remote Ethernet port that prevents the complete end-to-end Ethernet path from working. If any SONET path alarms such as the “AIS-P” alarm on page 2-31, the “LOP-P” alarm on page 2-145, the “PDI-P” alarm on page 2-201, or the “UNEQ-P” alarm on page 2-249 exist on the SONET path used by the Ethernet port, the affected port causes a TPTFAIL alarm. Also, if the remote-node G1000-4 port Ethernet port is administratively disabled or it is reporting the “CARLOSS (G1000)” alarm on page 2-58, the C2 byte in the SONET path overhead indicates the “PDI-P” alarm on page 2-201, which in turn causes a TPTFAIL to be reported against the local port.

When a TPTFAIL alarm occurs, the local port is automatically disabled (transmit laser turned off). In turn, the laser shutoff can also cause the external Ethernet device attached at the local node to detect a link down and turn off its transmitter. This also causes a CARLOSS alarm to occur on the reporting port. In all cases, the source problem is either in the SONET path being used by the G1000-4 port or the far-end G1000-4 port to which it is mapped.

An occurrence of TPTFAIL on an ONS 15454 G1000-4 port indicates either a problem with the SONET path that the port is using or with the remote-node G1000-4 port that is mapped to the port.

Clear the TPTFAIL (G1000) Alarm

-
- Step 1** Clear any alarms being reported by the OC-N card on the G1000-4 circuit.
- Step 2** If no alarms are reported by the OC-N card, or if the “PDI-P” condition on page 2-201 is reported, the problem could be on the remote-node G1000-4 port. Clear any alarms, such as CARLOSS, reported against the remote-node port or card.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.358 TPTFAIL (ML100T, ML1000)

- Default Severity: Major (MJ), Service-Affecting (SA)

- Logical Objects: ML100T, ML1000

The TPT Layer Failure alarm for the ML-Series Ethernet cards indicates a break in the end-to-end packet-over-SONET (POS) link integrity feature of the ML-Series POS cards. TPTFAIL indicates a remote-node condition or misconfiguration of the POS port.

The TPTFAIL alarm indicates a problem on the SONET path, a problem on the remote POS port, or a misconfiguration of the POS port that prevents the complete end-to-end POS path from working. If any SONET path alarms such as the “AIS-P” condition on page 2-31, the “LOP-P” alarm on page 2-145, the “PDI-P” condition on page 2-201, or the “UNEQ-P” alarm on page 2-249 exist on the circuit used by the POS port, the affected port could report a TPTFAIL alarm. If the remote-node ML POS port is administratively disabled, it inserts an “AIS-P” condition on page 2-31 that is detected by the local port. The local port could report TPTFAIL in this event. If the POS port is misconfigured at the Cisco IOS CLI level, the misconfiguration causes the port to go down and report TPTFAIL.

**Note**

For more information about the ML-Series Ethernet cards, refer to the *<I_Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the TPTFAIL (ML100T, ML1000) Alarm

-
- Step 1** If there are no SONET alarms reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *<I_Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for configuration information.
- Step 2** If the “PLM-P” alarm on page 2-204 is the only one reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *<I_Ital>Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for configuration information.
- Step 3** If the “PDI-P” condition on page 2-201 is the only one reported against the POS port circuit and the circuit is terminated by a G-Series card, determine whether a “CARLOSS (G1000)” alarm on page 2-58 is reported against the G-Series card, and if so, complete the “Clear the CARLOSS (G1000) Alarm” procedure on page 2-59.
- Step 4** If the “AIS-P” alarm on page 2-31, the “LOP-P” alarm on page 2-145, or the “UNEQ-P” alarm on page 2-249 is present, clear those alarms using the procedures in those sections.
- Step 5** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.359 TRMT

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

A Missing Transmitter alarm occurs when there is a transmit failure on the ONS 15454 DS-1 card because of an internal hardware failure. The card must be replaced.

Clear the TRMT Alarm

Step 1 Complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the reporting DS-1 card.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

Step 2 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.360 TRMT-MISS

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

A Facility Termination Equipment Transmitter Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance is detected when a transmit cable is missing on the DS-1 port or the backplane does not match the inserted card. For example, an SMB connector or a BNC connector might be connected to a DS-1 card instead of a DS-3 card.

**Note**

DS-1s are four-wire circuits and need a positive and negative connection for both transmit and receive.

Clear the TRMT-MISS Alarm

Step 1 Verify that the device attached to the DS-1 port is operational.

Step 2 If the device is operational, verify that the cabling is securely connected.

Step 3 If the cabling is secure, verify that the pinouts are correct.

Step 4 If the pinouts are correct, replace the transmit cable.

Step 5 If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

2.8.361 TX-AIS

- Default Severity: Not Reported (NR), Non-Service Affecting (NSA)

- Logical Objects: DS1, DS3

The (TX) Transmit Direction AIS condition is raised by the ONS 15454 backplane when it receives a remote-node DS-1 LOS.

Clear the TX-AIS Condition

-
- Step 1** Determine whether there are alarms on the downstream nodes and equipment, especially the “[LOS \(OCN\)](#)” alarm on page 2-153, or OOS ports.
- Step 2** Clear the downstream alarms using the applicable procedures in this chapter.
- Step 3** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.362 TX-RAI

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

The Transmit Direction RAI condition is transmitted by the backplane when it receives a DS-1 TX-AIS. This alarm is raised only at the transmit side, but RAI is raised at both ends.

Clear the TX-RAI Condition

-
- Step 1** Complete the “[Clear the TX-AIS Condition](#)” procedure on page 2-248.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.363 UNC-WORD

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Uncorrected FEC Word condition indicates that the forward error correction (FEC) capability could not sufficiently correct the frame.

FEC allows the system to tolerate a 7- to 8-dBm reduction in signal-to-noise ratio (SNR).

Clear the UNC-WORD Condition

-
- Step 1** Complete the “[Clear the SD-L Condition](#)” procedure on page 2-220.

- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.8.364 UNEQ-P

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: STSMON, STSTRM

An SLMF UNEQ Path alarm occurs when the path does not have a valid sender. The UNEQ-P indicator is carried in the C2 signal path byte in the SONET overhead. The source of the problem is the node that is transmitting the signal into the node reporting the UNEQ-P.

The alarm could result from a PARTIAL circuit or an empty VT tunnel. UNEQ-P occurs in the node that terminates a path.



Note

If a newly created circuit has no signal, an UNEQ-P alarm is reported on the OC-N cards and the “AIS-P” condition on page 2-31 is reported on the terminating cards. These alarms clear when the circuit carries a signal.



Caution

Deleting a circuit affects traffic.

Clear the UNEQ-P Alarm

- Step 1** In node view, click **View > Go to Network View**.
- Step 2** Right-click the alarm to display the Select Affected Circuits shortcut menu.
- Step 3** Click **Select Affected Circuits**.
- Step 4** When the affected circuits appear, look in the Type column for VTT, which indicates a VT tunnel circuit. A VT tunnel with no VTs assigned could be the cause of an UNEQ-P alarm.
- Step 5** If the Type column does not contain VTT, there are no VT tunnels connected with the alarm. Go to [Step 7](#).
- Step 6** If the Type column does contain VTT, attempt to delete these row(s):



Note

The node does not allow you to delete a valid VT tunnel or one with a valid VT circuit inside.

- Click the VT tunnel circuit row to highlight it. Complete the “Delete a Circuit” procedure on [page 2-272](#).
 - If an error message dialog box appears, the VT tunnel is valid and not the cause of the alarm.
 - If any other rows contain VTT, repeat [Step 6](#).
- Step 7** If all nodes in the ring appear in the CTC network view, determine whether the circuits are complete:
- Click the **Circuits** tab.
 - Verify that PARTIAL is not listed in the Status column of any circuits.

- Step 8** If you find circuits listed as PARTIAL, use an optical test set to verify that these circuits are not working circuits that continue to pass traffic.
- For specific procedures to use the test set equipment, consult the manufacturer.
- Step 9** If the PARTIAL circuits are not needed or are not passing traffic, delete the PARTIAL circuits.
- Complete the [“Delete a Circuit” procedure on page 2-272](#).
- Step 10** Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* Chapter 6, “Create Circuits and Tunnels.”
- Step 11** Log back in and verify that all circuits terminating in the reporting card are active:
- Click the **Circuits** tab.
 - Verify that the Status column lists all circuits as active.
- Step 12** If the alarm does not clear, clean the remote-node optical fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

**Warning**

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293

**Warning**

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056

**Warning**

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

**Caution**

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 13** If the alarm does not clear, complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the OC-N and DS-N cards.

**Caution**

Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the [“2.11.2 Protection Switching, Lock Initiation, and Clearing” section on page 2-260](#) for commonly used traffic-switching procedures.

**Note**

When you replace a card with an identical type of card, you do not need to make any changes to the database.

- Step 14** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.365 UNEQ-V

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Objects: VT-MON, VT-TERM

An SLMF UNEQ VT alarm indicates that the node is receiving SONET path overhead with Bits 5, 6, and 7 of the V5 overhead byte all set to zeroes. The source of the problem is the node that is transmitting the VT-level signal into the node reporting the UNEQ-V. The problem node is the next node upstream that processes the signal at the VT level. The V in UNEQ-V indicates that the failure has occurred at the VT layer.



Warning

On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0). Statement 293.



Warning

Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard. Statement 1056



Warning

Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure. Statement 1057

Clear the UNEQ-V Alarm

- Step 1** Complete the [“Clear the UNEQ-P Alarm” procedure on page 2-249](#).



Caution

Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.366 UNREACHABLE-TARGET-POWER

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Object: OCH

The Unreachable Port Target Power alarm occurs on WSS32 cards during startup as the card laser attains its correct power level. The condition disappears when the card successfully boots.

**Note**

UNREACHABLE-TARGET-POWER is an informational condition. It only requires troubleshooting if it does not clear.

2.8.367 UT-COMM-FAIL

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The Universal Transponder (UT) Module Communication Failure alarm is raised on MXP_2.5G_10E and TXP_MR_10E cards when there is a universal transponder communication failure because the UT has stopped responding to the TCC2/TCC2P.

Clear the UT-COMM-FAIL Alarm

-
- Step 1** Double-click the card to display the card view.
- Step 2** Request a laser restart:
- Click the **Maintenance > ALS** tabs.
 - Check the Request Laser Restart check box.
 - Click **Apply**.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.368 UT-FAIL

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The Universal Transponder Module Hardware Failure alarm is raised against MXP_2.5G_10E and TXP_MR_10E cards when a UT-COMM-FAIL alarm persists despite being reset.

Clear the UT-FAIL Alarm

-
- Step 1** Complete the [“Physically Replace a Traffic Card” procedure on page 2-271](#) for the alarmed card.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.369 VCG-DEG

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: VCG

The VCAT Group Degraded alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when one member circuit carried by the ML-Series Ethernet card is down. This alarm is accompanied by the “[OOU-TPT](#)” alarm on page 2-192. It only occurs when a critical alarm, such as LOS, causes a signal loss.

Clear the VCG-DEG Condition

-
- Step 1** Look for and clear any critical alarms that apply to the errored card, such as “[LOS \(2R\)](#)” alarm on page 2-147 or “[LOS \(OTS\)](#)” alarm on page 2-155.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.370 VCG-DOWN

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: VCG

The VCAT Group Down alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when both member circuits carried by the ML-Series Ethernet card are down. This alarm occurs in conjunction with another critical alarm, such as the “[LOS \(2R\)](#)” alarm on page 2-147.

Clear the VCG-DOWN Condition

-
- Step 1** Complete the “[Clear the VCG-DEG Condition](#)” procedure on page 2-253.
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.371 VOA-HDEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA High Degrade alarm is raised on DWDM cards when an equipped VOA exceeds the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the high degrade threshold. The alarmed card should be replaced at the next opportunity.

Clear the VOA-HDEG Alarm

-
- Step 1** Complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the alarmed card.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.372 VOA-HFAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA High Fail alarm is raised on DWDM cards when an equipped VOA exceeds the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the high fail threshold. The card must be replaced.

Clear the VOA-HFAIL Alarm

-
- Step 1** Complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the alarmed card.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.373 VOA-LDEG

- Default Severity: Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA Low Degrade alarm is raised on DWDM cards when an equipped VOA does not reach the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the low degrade threshold. The alarmed card should be replaced at the next opportunity.

Clear the VOA-LDEG Alarm

-
- Step 1** Complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the alarmed card.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.374 VOA-LFAIL

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA Low Fail alarm is raised on DWDM cards when an equipped VOA does not reach the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the low fail threshold. The card must be replaced.

Clear the VOA-LFAIL Alarm

-
- Step 1** Complete the “[Physically Replace a Traffic Card](#)” procedure on page 2-271 for the alarmed card.
- Step 2** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.8.375 VOLT-MISM

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: PWR

The Power Monitoring Mismatch Between Control Cards alarm is raised against the shelf when the power voltages of both TCC2/TCC2Ps are out of range of each other by more than 5Vdc.

Clear the VOLT-MISM Condition

-
- Step 1** Check the incoming voltage level to the shelf using a voltmeter. Follow site practices or consult the *Cisco ONS 15454 Procedure Guide* Chapter 1, “Install the Shelf and Backplane Cable,” for power installation procedures.
- Step 2** Correct any incoming voltage issues.
- Step 3** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.376 WKSWPR

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN, STSMON, TRUNK, VT-MON

The Working Switched To Protection condition occurs when a line experiences the “[LOS \(OCN\)](#)” alarm on page 2-153, the “[SD \(DS1, DS3\)](#)” condition on page 2-217, or the “[SD \(TRUNK\)](#)” condition on page 2-219.

Clear the WKSWPR Condition

-
- Step 1** Complete the [“Clear the LOS \(OCN\) Alarm” procedure on page 2-153](#).
- Step 2** If the condition does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.8.377 WTR

- Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN, STSMON, TRUNK, VT-MON

The Wait To Restore condition occurs when the [“WKSWPR” condition on page 2-255](#) is raised, but the wait-to-restore time has not expired, meaning that the active protect path cannot revert to the working path. The condition clears when the timer expires and traffic is switched back to the working path.



Caution

DS-1 traffic loss can occur on a DS-1 with 1:N protection if a DS-1 card is reset with the protect card in the WTR state.



Note

WTR is an informational condition and does not require troubleshooting.

2.8.378 WVL-MISMATCH

- Default Severity: Major (MJ), Service-Affecting (SA)
- Logical Object: TRUNK

The Equipment Wavelength Mismatch alarm applies to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. It occurs when you provision the card in CTC with a wavelength that the card does not support.

Clear the WVL-MISMATCH alarm

-
- Step 1** In node view, double-click the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, or MXP_2.5G_10G card to display the card view.
- Step 2** Click the **Provisioning > Card** tabs.
- Step 3** In the Wavelength field, view the provisioned card wavelength.
- Step 4** If you have access to the site, compare the wavelength listed on the card faceplate with the provisioned wavelength. If you are remote, compare this wavelength with the card identification in the inventory:
- In node view, click the **Inventory** tab.
 - Locate the slot where the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, or MXP_2.5G_10G card is installed and view the card wavelength in the name.

- Step 5** If the card was provisioned for the wrong wavelength, double-click the card in node view to display the card view.
 - Step 6** Click the **Provisioning > Card** tabs.
 - Step 7** In the Wavelength field, click the drop-down list and choose the correct wavelength.
 - Step 8** Click **Apply**.
 - Step 9** If the alarm does not clear, log into the Technical Support Website at <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.
-

2.9 DWDM Card LED Activity

ONS 15454 DWDM card LED activity differs from typical traffic card LED activity. The following sections list the DWDM card LED sequences during card insertion and reset.

2.9.1 DWDM Card LED Activity After Insertion

When an DWDM card is inserted in the shelf, the following LED activities occur:

1. The FAIL LED illuminates for approximately 35 seconds.
2. The FAIL LED blinks for approximately 40 seconds.
3. All LEDs illuminate and then turn off within 5 seconds.
4. If new software is being downloaded to the card, the ACT and SF LEDs blink for 20 seconds to 3.5 minutes, depending on the card type.
5. The ACT LED illuminates.
6. The SF LED stays illuminated until all card ports connect to their remote-node counterparts and a signal is present.

2.9.2 DWDM Card LED Activity During Reset

When an DWDM card resets (by software or hardware), the following LED activities occur:

1. The FAIL LED switches on for few seconds.
2. The FAIL LED on the physical card blinks and turns off.
3. The white LED with the letters “LDG” appears on the reset card in CTC.
4. The green ACT LED appears in CTC.

2.10 Traffic Card LED Activity

ONS 15454 traffic card LED behavior patterns are listed in the following sections. These sections give behavior for card insertion, reset, and side-switch.

2.10.1 Typical Traffic Card LED Activity After Insertion

When a non-DWDM card is inserted, the following LED activities occur:

1. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds.
2. The red FAIL LED blinks for 35 to 45 seconds.
3. All LEDs blink once and turn off for 5 to 10 seconds.
4. The ACT or ACT/SBY LED turns on. The SF LED can persist until all card ports connect to their remote-node counterparts and a signal is present.

2.10.2 Typical Traffic Card LED Activity During Reset

While a non-DWDM card resets, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.
2. The white LED with the letters “LDG” appears on the reset card in CTC.
3. The green ACT LED appears in CTC.

2.10.3 Typical Card LED State After Successful Reset

When a non-DWDM card successfully resets, the following LED states are present:

- If you are looking at the physical ONS 15454, the ACT/SBY LED is illuminated.
- If you are looking at node view of the ONS 15454, the current standby card has an amber LED depiction with the initials “SBY,” and this has replaced the white “LDG” depiction on the card in CTC.
- If you are looking at node view of the ONS 15454, the current active card has a green LED depiction with the initials “ACT,” and this has replaced the white “LDG” depiction on the card in CTC.

2.10.4 Typical Cross-Connect LED Activity During Side Switch

While an XC10G cross-connect card is switched in CTC from active (ACT) to standby (SBY) or vice versa, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.
2. The standby card yellow SBY LED becomes a green ACT LED, indicating it is now active.
3. The active card green ACT LED becomes a yellow SBY LED, indicating it is now standby.

2.11 Frequently Used Alarm Troubleshooting Procedures

This section gives common procedures that are frequently used when troubleshooting alarms. Most of these procedures are summarized versions of fuller procedures existing elsewhere in the ONS 15454 documentation. They are included in this chapter for the user’s convenience. For further information, please refer to the *Cisco ONS 15454 Procedure Guide*.

2.11.1 Node and Ring Identification, Change, Visibility, and Termination

The following procedures relate how to identify or change BLSR names and node IDs, and how to verify visibility from other nodes.

Identify a BLSR Ring Name or Node ID Number

-
- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
 - Step 2** In node view, click **View > Go to Network View**.
 - Step 3** Click the **Provisioning > BLSR** tabs.
 - Step 4** From the Ring Name column, record the ring name, or in the Nodes column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name.
-



Note For more information about ring or node traffic switching operations, refer to the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

Change a BLSR Ring Name

-
- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
 - Step 2** In node view, click **View > Go to Network View**.
 - Step 3** Click the **Provisioning > BLSR** tabs.
 - Step 4** Highlight the ring and click **Edit**.
 - Step 5** In the BLSR window, enter the new name in the Ring Name field.
 - Step 6** Click **Apply**.
 - Step 7** Click **Yes** in the Changing Ring Name dialog box.
-

Change a BLSR Node ID Number

-
- Step 1** Log into a node on the network. If you are already logged in, go to [Step 2](#).
 - Step 2** In node view, click **View > Go to Network View**.
 - Step 3** Click the **Provisioning > BLSR** tabs.
 - Step 4** Highlight the ring and click **Edit**.
 - Step 5** In the BLSR window, right-click the node on the ring map.
 - Step 6** Select **Set Node ID** from the shortcut menu.
 - Step 7** In the Edit Node ID dialog box, enter the new ID. The Node ID is the number in parentheses after the Node Name.

Step 8 Click **OK**.

Verify Node Visibility for Other Nodes

- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** In node view, click the **Provisioning > BLSR** tabs.
- Step 3** Highlight a BLSR.
- Step 4** Click **Ring Map**.
- Step 5** In the BLSR Ring Map window, verify that each node in the ring appears on the ring map with a node ID and IP address.
- Step 6** Click **Close**.
-

2.11.2 Protection Switching, Lock Initiation, and Clearing

The following sections give instructions for port, ring, and span switching and switch-clearing commands, as well as lock-ons and lockouts.

Initiate a 1+1 Protection Port Force Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Force switch.



Caution

The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.



Caution

Traffic is not protected during a Force protection switch.



Note

A Force command switches traffic on a working path even if the path has signal degrade (SD) or signal fail (SF) conditions. A Force switch does not switch traffic on a protect path. A Force switch preempts a Manual switch.

- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, select the protection group with the port you want to switch.
- Step 3** In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the Protect/Standby port, click this port.
- Step 4** In the Switch Commands area, click **Force**.
- Step 5** Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group says “Force to working” in the Selected Groups area.

Initiate a 1+1 Protection Port Manual Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Manual switch.



Note A Manual command switches traffic if the path has an error rate less than the signal degrade. A Manual switch is preempted by a Force switch.

- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, select the protection group with the port you want to switch.
- Step 3** In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the protect/standby port, click this port.
- Step 4** In the Switch Commands area, click **Manual**.
- Step 5** Click **Yes** in the Confirm Force Operation dialog box.
- Step 6** If the switch is successful, the group now says “Manual to working” in the Selected Groups area.
-

Clear a 1+1 Protection Port Force or Manual Switch Command



Note If the 1+1 protection group is configured as revertive, clearing a Force switch to protect (or working) moves traffic back to the working port. In revertive operation, the traffic always switches back to working. There is no revert to protect. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.



Note If the Force Switch was user-initiated, the reversion occurs immediately when the clear command is issued. The five-minute WTR period is not needed in this case. If the Force was system-initiated, allow the five-minute waiting period (during WTR) before the reversion occurs.

- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups area, choose the protection group containing the port you want to clear.
- Step 3** In the Selected Group area, choose the port you want to clear.
- Step 4** In the Switching Commands area, click **Clear**.
- Step 5** Click **Yes** in the Confirmation Dialog box.
- The Force switch is cleared. Traffic immediately reverts to the working port if the group was configured for revertive switching.
-

Initiate a Card or Port Lock On Command



Note

For 1:1 and 1:N electrical protection groups, working or protect cards can be placed in the Lock On state. For a 1+1 optical protection group, only the working port can be placed in the Lock On state.

-
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups list, click the protection group where you want to apply a lock-on.
- Step 3** If you determine that the protect card is in standby mode and you want to apply the lock-on to the protect card, make the protect card active if necessary:
- a. In the Selected Group list, click the protect card.
 - b. In the Switch Commands area, click **Force**.
- Step 4** In the Selected Group list, click the active card where you want to lock traffic.
- Step 5** In the Inhibit Switching area, click **Lock On**.
- Step 6** Click **Yes** in the confirmation dialog box.
-

Initiate a Card or Port Lock Out Command



Note

For 1:1 or 1:N electrical protection groups, working or protect cards can be placed in the Lock Out state. For a 1+1 optical protection group, only the protect port can be placed in the Lock Out state.

-
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups list, click the protection group that contains the card you want to lockout.
- Step 3** In the Selected Group list, click the card you want to lock traffic out of.
- Step 4** In the Inhibit Switching area, click **Lock Out**.
- Step 5** Click **Yes** in the confirmation dialog box.
- The lockout has been applied and traffic is switched to the opposite card.
-

Clear a Card or Port Lock On or Lock Out Command

-
- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** In the Protection Groups list, click the protection group that contains the card you want to clear.
- Step 3** In the Selected Group list, click the card you want to clear.
- Step 4** In the Inhibit Switching area, click **Unlock**.
- Step 5** Click **Yes** in the confirmation dialog box.

The lock-on or lockout is cleared.

Initiate a 1:1 Card Switch Command

**Note**

The Switch command only works on the Active card, whether it is Working or Protect. It does not work on the Standby card.

- Step 1** In node view, click the **Maintenance > Protection** tabs.
- Step 2** Click the protection group that contains the card you want to switch.
- Step 3** Under Selected Group, click the active card.
- Step 4** Next to Switch Commands, click **Switch**.
- The working slot should change to Working/Active and the protect slot should change to Protect/Standby.
-

Initiate a Force Switch for All Circuits on a Path Protection Span

This procedure forces all circuits in a path protection from the working span to the protect. It is used to remove traffic from a card that originates or terminates path protection circuits.

**Caution**

The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

**Caution**

Traffic is not protected during a Force protection switch.

- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 3](#).
- Step 2** Click **View > Go to Network View**.
- Step 3** Right-click a network span and choose **Circuits**.
- The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.
- Step 4** Click the **Perform UPSR span switching** field.
- Step 5** Choose **Force Switch Away** from the drop-down list.
- Step 6** Click **Apply**.
- Step 7** In the Confirm UPSR Switch dialog box, click **Yes**.
- Step 8** In the Protection Switch Result dialog box, click **OK**.
- In the Circuits on Span dialog box, the switch state for all circuits is FORCE. Unprotected circuits do not switch.
-

Initiate a Manual Switch for All Circuits on a Path Protection Span

This procedure manually switches all circuits in a path protection from the working span to the protect. It is used to remove traffic from a card that originates or terminates path protection circuits.



Caution

The Manual command does not override normal protective switching mechanisms.

Step 1 Log into a node on the network. If you are already logged in, continue with [Step 2](#).

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Click the **Perform UPSR span switching** field.

Step 4 Choose **Manual** from the drop-down list.

Step 5 Click **Apply**.

Step 6 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 7 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is Manual. Unprotected circuits do not switch.

Initiate a Lock Out of Protect-Switch for All Circuits on a Path Protection Span

This procedure prevents all circuits in a path protection working span from switching to the protect span. It is used to keep traffic off cards that originate or terminate path protection circuits.



Caution

The Lock Out of Protect command does not override normal protective switching mechanisms.

Step 1 Log into a node on the network. If you are already logged in, continue with [Step 2](#).

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Click the **Perform UPSR span switching** field.

Step 4 Choose **Lock Out of Protect** from the drop-down list.

Step 5 Click **Apply**.

Step 6 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 7 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is FORCE. Unprotected circuits do not switch.

Clear a Path Protection Span External Switching Command

**Note**

If the ports terminating a span are configured as revertive, clearing a Force switch to protect (or working) moves traffic back to the working port. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.

Step 1 Log into a node on the network. If you are already logged in, continue with [Step 2](#).

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Initiate a Force switch for all circuits on the span:

- a. Click the **Perform UPSR span switching** field.
- b. Choose **Clear** from the drop-down list.
- c. Click **Apply**.
- d. In the Confirm UPSR Switch dialog box, click **Yes**.
- e. In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is Clear. Unprotected circuits do not switch.

Initiate a Force Ring Switch on a BLSR

Step 1 Log into a node on the network. If you are already logged in, continue with [Step 2](#).

Step 2 From the View menu choose **Go to Network View**.

Step 3 In network view, click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR you are switching, then click **Edit**.

Step 5 Right-click a BLSR node west port and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **Force Ring** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

Initiate a Force Span Switch on a Four-Fiber BLSR

Step 1 Log into a node on the network. If you are already logged in, continue with [Step 2](#).

Step 2 From the View menu choose **Go to Network View**.

Step 3 In network view, click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR you are switching, then click **Edit**.

- Step 5** Right-click a BLSR node west port and choose **Set West Protection Operation**.
 - Step 6** In the Set West Protection Operation dialog box, choose **Force Span** from the drop-down list.
 - Step 7** Click **OK**.
 - Step 8** Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.
-

Initiate a Manual Ring Switch on a BLSR

- Step 1** From the View menu, choose **Go to Network View**.
 - Step 2** Click the **Provisioning > BLSR** tabs.
 - Step 3** Choose the BLSR and click **Edit**.
 - Step 4** Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).
 - Step 5** In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **Manual Ring** from the drop-down list.
 - Step 6** Click **OK**.
 - Step 7** Click **Yes** in the two Confirm BLSR Operation dialog boxes.
-

Initiate a Lock Out on a BLSR Protect Span

- Step 1** From the View menu choose **Go to Network View**.
 - Step 2** Click the **Provisioning > BLSR** tabs.
 - Step 3** Choose the BLSR and click **Edit**.
 - Step 4** Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).
 - Step 5** In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **Lockout Protect Span** from the drop-down list.
 - Step 6** Click **OK**.
 - Step 7** Click **Yes** in the two Confirm BLSR Operation dialog boxes.
-

Initiate an Exercise Ring Switch on a BLSR

- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** Click **View > Go to Network View**.
- Step 3** Click the **Provisioning > BLSR** tabs.
- Step 4** Click the row of the BLSR you are exercising, then click **Edit**.
- Step 5** Right-click the west port of a node and choose **Set West Protection Operation**.

- Step 6** In the Set West Protection Operation dialog box, choose **Exercise Ring** from the drop-down list.
 - Step 7** Click **OK**.
 - Step 8** Click **Yes** in the Confirm BLSR Operation dialog box.
-

Initiate an Exercise Ring Switch on a Four Fiber BLSR

- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
 - Step 2** Click **View > Go to Network View**.
 - Step 3** Click the **Provisioning > BLSR** tabs.
 - Step 4** Click the row of the BLSR you are exercising, then click **Edit**.
 - Step 5** Right-click the west port of a node and choose **Set West Protection Operation**.
 - Step 6** In the Set West Protection Operation dialog box, choose **Exercise Span** from the drop-down list.
 - Step 7** Click **OK**.
 - Step 8** Click **Yes** in the Confirm BLSR Operation dialog box.
-

Clear a BLSR External Switching Command

- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
 - Step 2** Click **View > Go to Network View**.
 - Step 3** Click the **Provisioning > BLSR** tabs.
 - Step 4** Click the BLSR you want to clear.
 - Step 5** Right-click the west port of the BLSR node where you invoked the switch and choose **Set West Protection Operation**.
 - Step 6** In the Set West Protection Operation dialog box, choose **Clear** from the drop-down list.
 - Step 7** Click **OK**.
 - Step 8** Click **Yes** in the Confirm BLSR Operation dialog box.
-

2.11.3 CTC Card Resetting and Switching

This section gives instructions for resetting traffic cards, TCC2/TCC2P cards, and cross-connect cards.



Caution

For TXP and MXP cards placed in a Y-cable protection group, do not perform a software reset on both cards simultaneously. Doing so will cause a traffic hit of more than one minute. For more information about Y-cable protection groups, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Caution**

Resetting the active card in a Y-cable group will cause a traffic outage if the standby card is down for any reason.

Reset a Traffic Card in CTC

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** In node view, position the cursor over the optical or electrical traffic card slot reporting the alarm.
- Step 3** Right-click the card. Choose **Reset Card** from the shortcut menu.
- Step 4** Click **Yes** in the Resetting Card dialog box.
-

Reset an Active TCC2/TCC2P and Activate the Standby Card

**Caution**

Resetting an active TCC2/TCC2P card reset can be traffic-affecting.

**Note**

Before you reset the TCC2/TCC2P, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** Identify the active TCC2/TCC2P card:
If you are looking at the physical ONS 15454 shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.
- Step 3** Right-click the active TCC2/TCC2P in CTC.
- Step 4** Choose **Reset Card** from the shortcut menu.
- Step 5** Click **Yes** in the Confirmation Dialog box.
The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.
- Step 6** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the [“2.10.3 Typical Card LED State After Successful Reset”](#) section on page 2-258.
- Step 7** Double-click the node and ensure that the reset TCC2/TCC2P is in standby mode and that the other TCC2/TCC2P is active. Verify the following:
- If you are looking at the physical ONS 15454 shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.
 - No new alarms appear in the Alarms window in CTC.
-

Side Switch the Active and Standby XC10G Cross-Connect Cards


Caution

The cross-connect card side switch is usually traffic-affecting.

Step 1 Log into a node on the network. For instructions regarding how to log into a node, refer *Cisco ONS 15454 Procedure Guide, Release 8.0*. If you are already logged in, continue with [Step 2](#).

Step 2 Display node view.

Step 3 Determine the active or standby XC10G cross-connect card.

The ACT/SBY LED of the active card is green. The ACT/SBY LED of the standby card is amber.


Note

You can also position the cursor over the card graphic to display a popup identifying the card as active or standby.

Step 4 In node view, click the **Maintenance > Cross-Connect > Cards** tabs.

Step 5 Click **Switch**.

Step 6 Click **Yes** in the Confirm Switch dialog box. See the “[2.10.4 Typical Cross-Connect LED Activity During Side Switch](#)” section on [page 2-258](#) for LED information.


Note

During a maintenance side switch or soft reset of an active XC10G card, the 1+1 protection group might display a protection switch. To disallow the protection switch from being displayed, the protection group should be locked at the node where XC switch or soft reset of an active XC switch is in progress.


Caution

Active cross connect (XC10G/XCVT) cards should not be physically removed.

The following rules must be followed for removing an Active Cross Connect Card (XC10G/XCVT):

If the active cross connect has to be removed, perform an XCVT/XC10G side switch to change the status of the card from active to standby and then remove the cross connect card once it goes back to standby.

OR

Perform a lockout on all circuits that originate from the node whose active cross connect card has to be removed (performing a lockout on all spans will also accomplish the same goal).

2.11.4 Physical Card Reseating, Resetting, and Replacement

This section gives instructions for physically reseating and replacing TCC2/TCC2P, cross-connect, and traffic cards.

**Caution**

Do not physically replace a card without first making provisions to switch or move traffic to a different card or circuit. General procedures for this are located in the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260. In-depth traffic switching procedures and information can be found in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card

**Caution**

Do not perform this action without the supervision and direction of Cisco TAC (1 800 553-2447).

**Caution**

The TCC2/TCC2P reseat might be traffic-affecting. Refer to the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for traffic-switching procedures.

**Note**

Before you reset the TCC2/TCC2P card, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

**Note**

When a standby TSC card is removed and reinserted (reseated), all three fan lights might momentarily illuminate, indicating that the fan TCC2/TCC2Ps have also reset.

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
Ensure that the TCC2/TCC2P you want to reseat is in standby mode. A standby card has an amber ACT/SBY (Active/Standby) LED illuminated.
- Step 2** When the TCC2/TCC2P is in standby mode, unlatch both the top and bottom ejectors on the TCC2/TCC2P.
- Step 3** Physically pull the card at least partly out of the slot until the lighted LEDs turn off.
- Step 4** Wait 30 seconds. Reinsert the card and close the ejectors.

**Note**

The TCC2/TCC2P requires several minutes to reboot and display the amber standby LED after rebooting. Refer to the *Cisco ONS 15454 Reference Manual* for more information about LED behavior during card rebooting.

Remove and Reinsert (Reseat) Any Card

-
- Step 1** Open the card ejectors.
- Step 2** Slide the card halfway out of the slot along the guide rails.
- Step 3** Slide the card all the way back into the slot along the guide rails.

Step 4 Close the ejectors.

Physically Replace a Traffic Card



Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for commonly used traffic-switching procedures.

- Step 1** Open the card ejectors.
- Step 2** Slide the card out of the slot.
- Step 3** Open the ejectors on the replacement card.
- Step 4** Slide the replacement card into the slot along the guide rails.
- Step 5** Close the ejectors.
-

Physically Replace an In-Service Cross-Connect Card



Caution The cross-connect reseal might be traffic-affecting. Refer to the “[2.11.2 Protection Switching, Lock Initiation, and Clearing](#)” section on page 2-260 for traffic-switching procedures prior to completing this procedure.



Note This procedure is placed in the chapter as a quick guide for the user’s convenience. An in-depth procedure is located in the *Cisco ONS 15454 Procedure Guide* Chapter 15, “Maintain the Node.”

- Step 1** Determine the active cross-connect card (XCVT/XC10G). The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is amber.



Note You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

- Step 2** Switch the active cross-connect card (XCVT/XC10G) to standby:
- In the node view, click the **Maintenance > Cross-Connect** tabs.
 - Under Cross Connect Cards, choose **Switch**.
 - Click **Yes** in the Confirm Switch dialog box.



Note After the active XCVT/XC10G goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

Step 3 Physically remove the new standby cross-connect card (XCVT/XC10G) from the ONS 15454.



Note An improper removal (IMPROPRMVL) alarm is raised when a card reseal is performed, unless the card is first deleted in Cisco Transport Controller (CTC). The alarm clears after the card replacement is complete.

Step 4 Insert the replacement cross-connect card (XCVT/XC10G) into the empty slot.
The replacement card boots up and becomes ready for service after approximately one minute.

2.11.5 Generic Signal and Circuit Procedures

This section gives instructions for verify BER thresholds, deleting circuits, provisioning SDCC terminations, and clearing loopbacks.

Verify the Signal BER Threshold Level

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
 - Step 2** In node view, double-click the card reporting the alarm to display the card view.
 - Step 3** Click the **Provisioning > Line** tabs.
 - Step 4** Under the **SD BER** (or **SF BER**) column on the Provisioning window, verify that the cell entry is consistent with the originally provisioned threshold. The default setting is 1E-7.
 - Step 5** If the entry is consistent with the original provisioning, go back to your original procedure.
 - Step 6** If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the original entry.
 - Step 7** Click **Apply**.
-

Delete a Circuit

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
 - Step 2** In node view, click the **Circuits** tab.
 - Step 3** Click the circuit row to highlight it and click **Delete**.
 - Step 4** Click **Yes** in the Delete Circuits dialog box.
-

Verify or Create Node Section DCC Terminations



Note Portions of this procedure are different for ONS 15454 DWDM nodes.

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** In node view, click the **Provisioning > Comm Channels > SDCC** tab.
- Step 3** View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to [Step 4](#).
- Step 4** If necessary, create a DCC termination:
- Click **Create**.
 - In the Create SDCC Terminations dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the Shift key.
 - In the port state area, click the **Set to IS** radio button.
 - Verify that the Disable OSPF on Link check box is unchecked.
 - Click **OK**.
-

Clear an OC-N Card Facility or Terminal Loopback Circuit

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** Double-click the reporting card in CTC to display the card view.
- Step 3** Click the **Maintenance > Loopback > Port** tabs.
- Step 4** In the Loopback Type column, determine whether any port row shows a state other than None.
- Step 5** If a row contains another state besides None, click in the column cell to display the drop-down list and select None.
- Step 6** In the Admin State column, determine whether any port row shows a state other than IS.
- Step 7** If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.
- Step 8** Click **Apply**.
-

Clear an OC-N Card Cross-Connect (XC) Loopback Circuit

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** Double-click the reporting card in CTC to display the card view.
- Step 3** Click the **Maintenance > Loopback > SONET STS** tabs.
- Step 4** Uncheck the XC Loopback check box.
- Step 5** Click **Apply**.
-

Clear a DS3XM-6 or DS3XM-12 Card Loopback Circuit

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).

- Step 2** Double-click the reporting card in CTC to display the card view.
 - Step 3** Click the **Maintenance > DS3** tabs or the **Maintenance > DS1** tabs.
 - Step 4** In the Loopback Type column, determine whether any port row shows a state other than None.
 - Step 5** If a row contains another state besides None, click in the column cell to display the drop-down list and select None.
 - Step 6** In the Admin State column, determine whether any port row shows a state other than IS.
 - Step 7** If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.
 - Step 8** Click **Apply**.
-

Clear Other DS-N Card, EC-1, or G1000 Card Loopbacks



Note This procedure does not apply to DS3XM-6 or DS3XM-12 cards.

- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
 - Step 2** Double-click the reporting card in CTC to display the card view.
 - Step 3** Click the **Maintenance > Loopback** tabs.
 - Step 4** In the Loopback Type column, determine whether any port row shows a state other than None.
 - Step 5** If a row contains another state besides None, click in the column cell to display the drop-down list and select **None**.
 - Step 6** In the Admin State column, determine whether any port row shows a state other than IS.
 - Step 7** If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.
 - Step 8** Click **Apply**.
-

Clear an MXP, TXP, or FC_MR Card Loopback Circuit

- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** Double-click the reporting card in CTC to display the card view.
- Step 3** Click the **Maintenance > Loopback** tabs.
- Step 4** In the Loopback Type column, determine whether any port row shows a state other than None.
- Step 5** If a row contains another state besides None, click in the column cell to display the drop-down list and select None.
- Step 6** In the Admin State column, determine whether any port row shows an admin state other than IS, for example, OOS,MT.
- Step 7** If a row shows an admin state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

Clear an Ethernet Card Loopback Circuit

This procedure applies to CE_100T-8 cards.

- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
- Step 2** Double-click the reporting card in CTC to display the card view.
- Step 3** Click the **Maintenance > Loopback** tabs.
- Step 4** In the Loopback Type column, determine whether any port row shows a state other than None.
- Step 5** If a row contains another state besides None, click in the column cell to display the drop-down list and select **None**.
- Step 6** In the Admin State column, determine whether any port row shows a state other than IS, for example, OOS,MT.
- Step 7** If a row shows an Admin State other than IS, click in the column cell to display the drop-down list and select **IS**.
- Step 8** Click **Apply**.
-

2.11.6 Air Filter and Fan Procedures

This section gives instructions for cleaning or replacing the air filter and reseating or replacing the fan tray assembly.

Inspect, Clean, and Replace the Reusable Air Filter

To complete this task, you need a vacuum cleaner or detergent and water faucet, a spare filter, and a pinned hex key.



Warning

Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard. Statement 206

Although the filter works if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

- Step 1** Verify that you are replacing a reusable air filter. The reusable filter is made of a gray, open-cell, polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS 15454 use a reusable air filter.
- Step 2** If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that might have collected on the filter. If the filter is installed beneath the fan tray and not in the external filter brackets, open and remove the front door assembly:
- Open the front door of the shelf assembly. If it is already open or if the shelf assembly does not have a front door, continue with [Step 3](#).

- Open the front door lock.
 - Press the door button to release the latch.
 - Swing the door open.
- b. Remove the front door (optional):
- Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
 - Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
 - Secure the dangling end of the ground strap to the door or chassis with tape.

Step 3 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 4 Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 5 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 6 Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that might have collected on the filter.

Step 7 Visually inspect the air filter material for dirt and dust.

Step 8 If the reusable air filter has a concentration of dirt and dust, either vacuum or wash the air filter. Prior to washing the air filter, replace the dirty air filter with a clean air filter and also reinsert the fan-tray assembly. Wash the dirty air filter under a faucet with a light detergent.

Spare ONS 15454 filters should be kept in stock for this purpose.



Note Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

Step 9 If you washed the filter, allow it to completely air dry for at least eight hours.



Caution Do not put a damp filter back in the ONS 15454.

Step 10 If the air filter should be installed in the external filter brackets, slide the air filter all the way to the back of the brackets to complete the procedure.

Step 11 If the filter should be installed beneath the fan-tray assembly, remove the fan-tray assembly and slide the air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.



Caution If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly.



Note On a powered-up ONS 15454, the fans start immediately after the fan-tray assembly is correctly inserted.

Step 12 To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

Step 13 Rotate the retractable handles back into their compartments.

- Step 14** Replace the door and reattach the ground strap.
-

Remove and Reinsert a Fan-Tray Assembly

- Step 1** Use the retractable handles embedded in the front of the fan-tray assembly to pull it forward several inches.
- Step 2** Push the fan-tray assembly firmly back into the ONS 15454.
- Step 3** Close the retractable handles.
-

Replace the Fan-Tray Assembly

**Caution**

The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 R3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857; 15454-SA-HD, P/N: 800-24848). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 R3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a incompatible shelf assembly.

**Caution**

Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the backplane.

**Note**

The 15454-SA-ANSI or 15454-SA-HD shelf assembly and 15454-FTA3 fan-tray assembly are required with the ONS 15454 OC-192 and OC-48 AS cards.

To replace the fan-tray assembly (FTA), it is not necessary to move any of the cable management facilities.

- Step 1** Open the front door of the shelf assembly. If the shelf assembly does not have a front door, continue with [Step 3](#).
- Open the front door lock.
 - Press the door button to release the latch.
 - Swing the door open.
- Step 2** Remove the front door (optional):
- Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
 - Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
 - Secure the dangling end of the ground strap to the door or chassis with tape.
- Step 3** Push the outer side of the handles on the fan-tray assembly to expose the handles.
- Step 4** Fold out the retractable handles at the outside edges of the fan tray.

- Step 5** Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.
- Step 6** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.
- Step 7** If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.
- If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime. For more information on the fan-tray air filter, see the [“Inspect, Clean, and Replace the Reusable Air Filter”](#) section on page 2-275.
- Step 8** Slide the new fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.
- Step 9** To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.
- Step 10** If you replace the door, be sure to reattach the ground strap.
-

2.11.7 Interface Procedures

This section includes instructions for replacing an ONS 15454 EIA and an ONS 15454 AIP.

Replace the Electrical Interface Assembly



Note

You need a #2 Phillips screwdriver. If you use high-density BNC EIAs, you also need a BNC insertion and removal tool.

- Step 1** To remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.
- Step 2** Loosen the nine perimeter screws that hold the backplane sheet metal cover or EIA in place. Do not remove the interior screws.



Note

If you are removing an AMP Champ EIA, remove the fastening plate before proceeding. To remove the fastening plate, loosen the two thumbscrews.

- Step 3** If a backplane cover is attached to the ONS 15454, lift the panel by the bottom to remove it from the shelf assembly and store the panel for later use.
- Step 4** If an EIA is attached to the ONS 15454, lift the EIA handles and gently pull it away from the backplane.



Note

Attach backplane sheet metal covers whenever EIAs are not installed.

- Step 5** Line up the connectors on the new EIA with the mating connectors on the backplane.
- Step 6** Gently push the EIA until both sets of connectors fit together snugly.
- Step 7** Replace the nine perimeter screws that you removed while removing the backplane cover.

- Step 8** If you are installing an AMP Champ EIA, attach the fastening plate with the two thumbscrews.
- Step 9** Reattach the lower backplane cover.
-

Replace the Alarm Interface Panel

**Caution**

Do not use a 2A AIP with a 5A fan-tray assembly; doing so causes a blown fuse on the AIP.

**Caution**

If any nodes in an Ethernet circuit are not using Software R4.0 or later, there is a risk of Ethernet traffic disruptions. Contact Cisco TAC at 1 800 553-2447 when prompted to do so in the procedure.

**Note**

Perform this procedure during a maintenance window. Resetting the active TCC2/TCC2P card can cause a service disruption of less than 50 ms to OC-N or DS-N traffic. Resetting the active TCC2/TCC2P card can cause a service disruption of 3 to 5 minutes on all Ethernet traffic due to spanning tree reconvergence if any nodes in the Ethernet circuit are not using Software R4.0 or later.

**Caution**

Do not perform this procedure on a node with live traffic. Hot-swapping the AIP can affect traffic and result in a loss of data. For assistance with AIP replacement contact Cisco TAC (1 800 553-2447).

This procedure replaces an existing AIP with a new AIP on an in-service node without affecting traffic. Ethernet circuits that traverse nodes with a software release prior to R4.0 is affected.

You need a #2 Phillips screwdriver.

- Step 1** Ensure that all nodes in the affected network are running the same software version before replacing the AIP and repairing circuits:
- In network view, click the **Maintenance > Software** tabs. The working software version for each node is listed in the Working Version column.
 - If you need to upgrade the software on a node, refer to the *Cisco ONS 15454 Software Upgrade Guide* for software upgrade procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to [Step 2](#).
- Step 2** Record the MAC address of the old AIP:
- Log into the node where you are replacing the AIP. For login procedures, see the *Cisco ONS 15454 Procedure Guide* Chapter 3, “Connect the PC and Log into the GUI.”
 - In node view, click the **Provisioning > Network** tabs.
 - Record the MAC address shown in the General tab.
- Step 3** Call Cisco TAC (1 800 553-2447) for assistance in replacing the AIP and maintaining the original MAC address.



Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

- Step 4** Unscrew the five screws that hold the lower backplane cover in place.
- Step 5** Grip the lower backplane cover and gently pull it away from the backplane.
- Step 6** Unscrew the two screws that hold the AIP cover in place.
- Step 7** Grip the cover and gently pull away from the backplane.



Note On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

- Step 8** Grip the AIP and gently pull it away from the backplane.
- Step 9** Disconnect the fan-tray assembly power cable from the AIP.
- Step 10** Set the old AIP aside for return to Cisco.



Caution The type of shelf the AIP resides in determines the version of AIP that should replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) and 15454-SA-HD (P/N: 800-24848) currently use the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and earlier use the 2A AIP (P/N: 73-5262-01).



Caution Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI (P/N: 800-19857) or 15454-SA-HD (P/N: 800-24848) shelf; doing so causes a blown fuse on the AIP.

- Step 11** Attach the fan-tray assembly power cable to the new AIP.
- Step 12** Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.
- Step 13** Replace the AIP cover over the AIP and secure the cover with the two screws.
- Step 14** Replace the lower backplane cover and secure the cover with the five screws.
- Step 15** In node view, click the **Provisioning > Network** tabs.



Caution Cisco recommends TCC2/TCC2P card resets be performed in a maintenance window to avoid any potential service disruptions.

- Step 16** Reset the standby TCC2/TCC2P card:
- a. Right-click the standby TCC2/TCC2P card and choose **Reset Card**.
 - b. Click **Yes** in the Resetting Card dialog box. As the card resets, a loading (Ldg) indication appears on the card in CTC.



Note The reset takes approximately five minutes. Do not perform any other steps until the reset is complete.

- Step 17** Reset the active TCC2/TCC2P card:
- Right click the active TCC2/TCC2P card and choose **Reset Card**.
 - Click **Yes** in the Resetting Card dialog box. As the card resets, a Ldg indication appears on the card in CTC.



Note The reset takes approximately five minutes and CTC loses its connection with the node.

- Step 18** From the **File** drop-down list, choose **Exit** to exit the CTC session.
- Step 19** Log back into the node. At the Login dialog box, choose **(None)** from the Additional Nodes drop-down list.
- Step 20** Record the new MAC address:
- In node view, click the **Provisioning > Network** tabs.
 - Record the MAC address shown in the General tab.
- Step 21** In node view, click the **Circuits** tab. Note that all circuits listed are PARTIAL.
- Step 22** In node view, choose **Repair Circuits** from the **Tools** drop-down list. The Circuit Repair dialog box appears.
- Step 23** Read the instructions in the Circuit Repair dialog box. If all the steps in the dialog box have been completed, click **Next**. Ensure that you have the old and new MAC addresses.
- Step 24** The Node MAC Addresses dialog box appears:
- From the Node drop-down list, choose the name of the node where you replaced the AIP.
 - In the Old MAC Address field, enter the old MAC address that was recorded in [Step 2](#).
 - Click **Next**.
- Step 25** The Repair Circuits dialog box appears. Read the information in the dialog box and click **Finish**.



Note The CTC session freezes until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned.

When the circuit repair is complete, the Circuits Repaired dialog box appears.

- Step 26** Click **OK**.
- Step 27** In the node view of the new node, click the **Circuits** tab. Note that all circuits listed are DISCOVERED. If all circuits listed do not have a DISCOVERED status, call the Cisco TAC (1 800 553-2447) to open a Return Material Authorization (RMA).
-

