



Alarm Troubleshooting

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco ONS 15454 alarm and condition. Tables 2-1 through 2-4 provide lists of ONS 15454 alarms organized by severity. Table 2-6 on page 2-6 provides a list of alarms organized alphabetically. Table 2-8 on page 2-11 provides a list of alarms organized by alarm type. For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.



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.

The troubleshooting procedure for an alarm applies to both the Cisco Transport Controller (CTC) and TL1 version of that alarm. If the troubleshooting procedure does not clear the alarm, log onto <http://www.cisco.com/techsupport> for more information or call the Cisco Technical Assistance Center (Cisco TAC) to report a service-affecting problem (1 800 553-2447).

For alarm profile information, refer to the *Cisco ONS 15454 Procedure Guide*.

2.1 Alarm Index by Default Severity

The following tables group alarms and conditions by the severity displayed in the CTC Alarms window in the severity (SEV) column, which is the same severity used when reported by TL1. All severities listed in this manual are the default profile settings. Alarm severities can be altered from default settings for individual alarms or groups of alarms by creating a nondefault alarm profile and applying it on a port, card, or shelf basis. All settings (default or user-defined) that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in Non-Service-Affecting (NSA) situations as defined in Telcordia GR-474.



Note

The CTC default alarm profile contains alarms that apply to multiple product platforms. The alarms that apply to this product are listed in the following tables and sections.

2.1.1 Critical Alarms (CR)

Table 2-1 lists Critical alarms.

Table 2-1 Critical Alarm Index

AUTOLSROFF, page 2-35	LOF (DS3), page 2-122	MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151
BKUPMEMP, page 2-42	LOF (EC1-12), page 2-123	OPWR-HFAIL, page 2-160
CKTDOWN, page 2-51	LOF (OCN), page 2-123	OPWR-LFAIL, page 2-161
COMIOXC, page 2-54	LOF (TRUNK), page 2-124	OTUK-LOF, page 2-162
CTNEQPT-PBPROT, page 2-59	LOM, page 2-124 for STSTRM, TRUNK	PLM-P, page 2-167
CTNEQPT-PBWORK, page 2-61	LOP-P, page 2-125 for STSMON, STSTRM	PORT-CODE-MISM, page 2-168
EQPT, page 2-69	LOS (CLIENT), page 2-127	PORT-COMM-FAIL, page 2-168
EQPT-MISS, page 2-70	LOS (DS3), page 2-129	PORT-MISMATCH, page 2-169 (for CLIENT only)
FAN, page 2-83	LOS (EC1-12), page 2-130	PORT-MISSING, page 2-169
GAIN-HFAIL, page 2-98	LOS (OCN), page 2-132	SQM, page 2-188 for STSTRM
GAIN-LFAIL, page 2-99	LOS (OTS), page 2-134	SWMTXMOD, page 2-193
GE-OOSYNC, page 2-100	LOS (TRUNK), page 2-135	TIM, page 2-198 (for CLIENT, TRUNK only)
HITEMP, page 2-103 (for NE only)	LOS-P, page 2-136	TIM-P, page 2-199, for STSTRM
I-HITEMP, page 2-105	MEA (AIP), page 2-148	UNEQ-P, page 2-204
IMPROPRMVL, page 2-105	MEA (EQPT), page 2-148	VOA-HFAIL, page 2-208
LOA, page 2-119	MEA (FAN), page 2-150	VOA-LFAIL, page 2-209
LOF (CLIENT), page 2-121	—	—

2.1.2 Major Alarms (MJ)

Table 2-2 lists Major alarms.

Table 2-2 Major Alarm Index

APC-DISABLED, page 2-24	DUP-IPADDR, page 2-65	LOS (BITS), page 2-127
APC-FAIL, page 2-25	DUP-NODENAME, page 2-65	LOS (DS1), page 2-128
APSCM, page 2-29	EHIBATVG, page 2-66	LWBATVG, page 2-145
APSCNMIS, page 2-30	ELWBATVG, page 2-66	MEM-GONE, page 2-151
AWG-FAIL, page 2-40	EOC, page 2-66	OPTNTWMIS, page 2-157
AWG-OVERTEMP, page 2-41	EOC-L, page 2-68	PEER-NORESPONSE, page 2-166
BAT-FAIL, page 2-41	E-W-MISMATCH, page 2-73	PLM-V, page 2-167
BLSROSYNC, page 2-43	EXTRA-TRAF-PREEMPT, page 2-77	PRC-DUPID, page 2-170

Table 2-2 Major Alarm Index (continued)

CARLOSS (CLIENT), page 2-43	FANDEGRADE, page 2-84	RCVR-MISS, page 2-173
CARLOSS (EQPT), page 2-44	FEC-MISM, page 2-84	RING-ID-MIS, page 2-176
CARLOSS (E100T, E1000F), page 2-45	GCC-EOC, page 2-100	RING-MISMATCH, page 2-176
CARLOSS (G1000), page 2-46	HIBATVG, page 2-100	SQM, page 2-188 for VT-TERM
CARLOSS (ML100T, ML1000), page 2-49	HLDOVRSYNC, page 2-104	SYSBOOT, page 2-197
CARLOSS (TRUNK), page 2-50	INC-SIGLOSS, page 2-109	TPTFAIL (FC_MR-4), page 2-200
CONTBUS-A-18, page 2-55	INC-SYNCLOSS, page 2-110	TPTFAIL (G1000), page 2-200
CONTBUS-B-18, page 2-55	INVMACADR, page 2-111	TPTFAIL (ML100T, ML1000), page 2-201
CONTBUS-IO-A, page 2-56	LOF (BITS), page 2-120	TRMT, page 2-201
CONTBUS-IO-B, page 2-57	LOF (DS1), page 2-121	TRMT-MISS, page 2-202
DBOSYNC, page 2-62	LOM, page 2-124 for VT-TERM	UNEQ-V, page 2-206
DSP-COMM-FAIL, page 2-63	LOP-V, page 2-125	WVL-MISMATCH, page 2-210
DSP-FAIL, page 2-63	—	—

2.1.3 Minor Alarms (MN)

Table 2-3 lists Minor alarms.

Table 2-3 Minor Alarm Index

APSB, page 2-26	GAIN-LDEG, page 2-98	OPWR-LDEG, page 2-160
APSCDFLTK, page 2-27	HI-LASERBIAS, page 2-101	PROTNA, page 2-170
APSC-IMP, page 2-28	HI-RXPOWER, page 2-102	PTIM, page 2-171
APSCINCON, page 2-29	HITEMP, page 2-103	PWR-REDUN, page 2-172
APSMM, page 2-32	HI-TXPOWER, page 2-103	RSVP-HELLODOWN, page 2-177
AUTORESET, page 2-36	KBYTE-APS-CHANNEL-FAILURE, page 2-114	SFTWDOWN, page 2-183
AUTOSW-LOP (VT-MON), page 2-37	LASERBIAS-DEG, page 2-115	SH-INS-LOSS-VAR-DEG-HIGH, page 2-183
AUTOSW-UNEQ (VT-MON), page 2-39	LASEREOL, page 2-116	SH-INS-LOSS-VAR-DEG-LOW, page 2-184
AWG-DEG, page 2-40	LASERTEMP-DEG, page 2-117	SNTP-HOST, page 2-185
CASETEMP-DEG, page 2-50	LMP-HELLODOWN, page 2-118	SSM-FAIL, page 2-189
COMM-FAIL, page 2-54	LMP-NDFAIL, page 2-118	SYNCPRI, page 2-195
DATAFLT, page 2-62	LO-RXPOWER, page 2-126	SYNCSEC, page 2-196
ERROR-CONFIG, page 2-72	LOS (FUDC), page 2-131	SYNCTHIRD, page 2-197
EXCCOL, page 2-75	LO-TXPOWER, page 2-137	TIM-MON, page 2-198
EXT, page 2-77	MEM-LOW, page 2-151	TIM-P, page 2-199, for STSMON

Table 2-3 Minor Alarm Index (continued)

FEPRLF, page 2-93	NOT-AUTHENTICATED, page 2-153	VOA-HDEG, page 2-207
FSTSYNC, page 2-97	OPTNTWMIS, page 2-157	VOA-LDEG, page 2-208
GAIN-HDEG, page 2-97	OPWR-HDEG, page 2-158	—

2.1.4 NA Conditions

Table 2-4 lists not alarmed (NA) conditions.

Table 2-4 NA Conditions Index

ALS, page 2-23	FRNGSYNC, page 2-96	OTUK-TIM, page 2-164
AMPLI-INIT, page 2-24	FULLPASSTHR-BI, page 2-97	OUT-OF-SYNC, page 2-164
APSIMP, page 2-31	INC-GFP-OUTOFFRAME, page 2-107	PDI-P, page 2-164
AS-CMD, page 2-32	INC-GFP-SIGLOSS, page 2-108	PORT-MISMATCH, page 2-169 for FC_MR-4
AS-MT, page 2-33	INC-GFP-SYNCLOSS, page 2-108	RAI, page 2-172
AUD-LOG-LOSS, page 2-34	INC-ISD, page 2-109	RING-SW-EAST, page 2-177
AUD-LOG-LOW, page 2-34	INHSWPR, page 2-110	RING-SW-WEST, page 2-177
AUTOSW-LOP (STSMON), page 2-37	INHSWWKG, page 2-110	RUNCFG-SAVENEED, page 2-178
AUTOSW-PDI, page 2-38	INTRUSION-PSWD, page 2-111	SD (CLIENT, TRUNK), page 2-178
AUTOSW-SDBER, page 2-38	IOSCFGCOPY, page 2-113	SD (DS1, DS3), page 2-178
AUTOSW-SFBER, page 2-38	KB-PASSTHR, page 2-114	SD-L, page 2-180
AUTOSW-UNEQ (STSMON), page 2-39	LAN-POL-REV, page 2-114	SD-P, page 2-180
AWG-WARM-UP, page 2-41	LASER-APR, page 2-115	SF (CLIENT, TRUNK), page 2-181
CLDRESTART, page 2-53	LASERBIAS-FAIL, page 2-116	SF (DS1, DS3), page 2-182
CTNEQPT-MISMATCH, page 2-58	LASEREOL, page 2-116	SF-L, page 2-182
DS3-MISM, page 2-64	LKOUTPR-S, page 2-118	SF-P, page 2-183
ETH-LINKLOSS, page 2-73	LOCKOUT-REQ, page 2-119	SHUTTER-OPEN, page 2-184
EXERCISE-RING-FAIL, page 2-76	LPBKCRS, page 2-138	SPAN-SW-EAST, page 2-185
EXERCISE-SPAN-FAIL, page 2-76	LPBKDS1FEAC, page 2-139	SPAN-SW-WEST, page 2-186
FAILTOSW, page 2-78	LPBKDS1FEAC-CMD, page 2-139	SQUELCH, page 2-186
FAILTOSW-PATH, page 2-79	LPBKDS3FEAC, page 2-139	SQUELCHED, page 2-187
FAILTOSWR, page 2-79	LPBKDS3FEAC-CMD, page 2-140	SSM-DUS, page 2-188
FAILTOSWS, page 2-81	LPBKFACILITY (CLIENT, TRUNK), page 2-140	SSM-LNC, page 2-189
FE-AIS, page 2-84	LPBKFACILITY (DS1, DS3), page 2-141	SSM-OFF, page 2-189

Table 2-4 NA Conditions Index (continued)

FE-DS1-MULTLOS, page 2-85	LPBKFACILITY (EC1-12), page 2-141	SSM-PRC, page 2-190
FE-DS1-NSA, page 2-85	LPBKFACILITY (G1000), page 2-142	SSM-PRS, page 2-190
FE-DS1-SA, page 2-86	LPBKFACILITY (OCN), page 2-142	SSM-RES, page 2-190
FE-DS1-SNGLLOS, page 2-86	LPBKTERMINAL (CLIENT, TRUNK), page 2-143	SSM-SMC, page 2-191
FE-DS3-NSA, page 2-87	LPBKTERMINAL (DS1, DS3, EC-1-12, OCN), page 2-144	SSM-STU, page 2-191
FE-DS3-SA, page 2-88	LPBKTERMINAL (G1000), page 2-144	SSM-ST2, page 2-191
FE-EQPT-NSA, page 2-88	MAN-REQ, page 2-145	SSM-ST3, page 2-192
FE-FRCDWKS WPR-RING, page 2-89	MANRESET, page 2-146	SSM-ST3E, page 2-192
FE-FRCDWKS WPR-SPAN, page 2-89	MANSWTOINT, page 2-146	SSM-ST4, page 2-192
FE-IDLE, page 2-90	MANSWTOPRI, page 2-146	SSM-TNC, page 2-192
FE-LOCKOUTOFPR-SPAN, page 2-90	MANSWTOSEC, page 2-146	SWTOPRI, page 2-194
FE-LOF, page 2-91	MANSWTO THIRD, page 2-147	SWTOSEC, page 2-194
FE-LOS, page 2-91	MANUAL-REQ-RING, page 2-147	SWTO THIRD, page 2-194
FE-MANWKS WPR-RING, page 2-92	MANUAL-REQ-SPAN, page 2-147	SYNC-FREQ, page 2-195
FE-MANWKS WPR-SPAN, page 2-92	NO-CONFIG, page 2-152	TIM, page 2-198 (for OCN only)
FORCED-REQ, page 2-94	ODUK-SD-PM, page 2-156	TX-RAI, page 2-203
FORCED-REQ-RING, page 2-94	ODUK-SF-PM, page 2-156	UNC-WORD, page 2-203
FORCED-REQ-SPAN, page 2-95	ODUK-TIM-PM, page 2-156	VCG-DEG, page 2-206
FRCDSWTOINT, page 2-95	OOU-TPT, page 2-157	VCG-DOWN, page 2-207
FRCDSWTOPRI, page 2-95	OTUK-SD, page 2-163	WKS WPR, page 2-209
FRCDSWTOSEC, page 2-96	OTUK-SF, page 2-163	WTR, page 2-210
FRCDSWTO THIRD, page 2-96	—	—

2.1.5 NR Conditions

Table 2-5 lists not reported (NR) conditions.

Table 2-5 NR Conditions Index

AIS, page 2-21	ERFI-P-SRVR, page 2-71	OTUK-BDI, page 2-162
AIS-L, page 2-22	ODUK-AIS-PM, page 2-154	RFI, page 2-173
AIS-P, page 2-22	ODUK-BDI-PM, page 2-154	RFI-L, page 2-174
AIS-V, page 2-23	ODUK-LCK-PM, page 2-155	RFI-P, page 2-174
AUTOSW-AIS, page 2-36	ODUK-OCI-PM, page 2-155	RFI-V, page 2-175
ERFI-P-CONN, page 2-71	OTUK-AIS, page 2-161	TX-AIS, page 2-203
ERFI-P-PAYLD, page 2-71	—	—

2.2 Alarms and Conditions Indexed By Alphabetical Entry

Table 2-6 lists alarms and conditions by the name displayed on the CTC Alarms window or Conditions window.

Table 2-6 *Alphabetical Alarm Index*

AIS, page 2-21	FRCDSWTOINT, page 2-95	ODUK-OCI-PM, page 2-155
AIS-L, page 2-22	FRCDSWTOPRI, page 2-95	ODUK-SD-PM, page 2-156
AIS-P, page 2-22	FRCDSWTOSEC, page 2-96	ODUK-SF-PM, page 2-156
AIS-V, page 2-23	FRCDSWTOTHIRD, page 2-96	ODUK-TIM-PM, page 2-156
ALS, page 2-23	FRNGSYNC, page 2-96	OOU-TPT, page 2-157
AMPLI-INIT, page 2-24	FSTSYNC, page 2-97	OPTNTWMIS, page 2-157
APC-DISABLED, page 2-24	FULLPASSTHR-BI, page 2-97	OPWR-HDEG, page 2-158
APC-FAIL, page 2-25	GAIN-HDEG, page 2-97	OPWR-HFAIL, page 2-160
APSB, page 2-26	GAIN-HFAIL, page 2-98	OPWR-LDEG, page 2-160
APSCDFLTK, page 2-27	GAIN-LDEG, page 2-98	OPWR-LFAIL, page 2-161
APSC-IMP, page 2-28	GAIN-LFAIL, page 2-99	OTUK-AIS, page 2-161
APSCINCON, page 2-29	GCC-EOC, page 2-100	OTUK-BDI, page 2-162
APSCM, page 2-29	GE-OOSYNC, page 2-100	OTUK-LOF, page 2-162
APSCNMIS, page 2-30	HIBATVG, page 2-100	OTUK-SD, page 2-163
APSIMP, page 2-31	HI-LASERBIAS, page 2-101	OTUK-SF, page 2-163
APSM, page 2-32	HI-RXPOWER, page 2-102	OTUK-TIM, page 2-164
AS-CMD, page 2-32	HITEMP, page 2-103	OUT-OF-SYNC, page 2-164
AS-MT, page 2-33	HI-TXPOWER, page 2-103	PDI-P, page 2-164
AUD-LOG-LOSS, page 2-34	HLDOVRSYNC, page 2-104	PEER-NORESPONSE, page 2-166
AUD-LOG-LOW, page 2-34	I-HITEMP, page 2-105	PLM-P, page 2-167
AU-LOF, page 2-34	IMPROPRMVL, page 2-105	PLM-V, page 2-167
AUTOLSROFF, page 2-35	INC-GFP-OUTOFFRAME, page 2-107	PORT-CODE-MISM, page 2-168
AUTORESET, page 2-36	INC-GFP-SIGLOSS, page 2-108	PORT-COMM-FAIL, page 2-168
AUTOSW-AIS, page 2-36	INC-GFP-SYNCLLOSS, page 2-108	PORT-MISMATCH, page 2-169
AUTOSW-LOP (STSMON), page 2-37	INC-ISD, page 2-109	PORT-MISSING, page 2-169
AUTOSW-LOP (VT-MON), page 2-37	INC-SIGLOSS, page 2-109	PRC-DUPID, page 2-170
AUTOSW-PDI, page 2-38	INC-SYNCLLOSS, page 2-110	PROTNA, page 2-170
AUTOSW-SDBER, page 2-38	INC-ISD, page 2-109	PTIM, page 2-171
AUTOSW-SFBER, page 2-38	INHWP, page 2-110	PWR-REDUN, page 2-172
AUTOSW-UNEQ (STSMON), page 2-39	INHWWKG, page 2-110	RAI, page 2-172
AUTOSW-UNEQ (VT-MON), page 2-39	INTRUSION-PSWD, page 2-111	RCVR-MISS, page 2-173
AWG-DEG, page 2-40	INVMACADR, page 2-111	RFI, page 2-173

Table 2-6 Alphabetical Alarm Index (continued)

AWG-FAIL, page 2-40	IOSCFGCOPY, page 2-113	RFI-L, page 2-174
AWG-OVERTEMP, page 2-41	KB-PASSTHR, page 2-114	RFI-P, page 2-174
AWG-WARM-UP, page 2-41	KBYTE-APS-CHANNEL-FAILURE, page 2-114	RFI-V, page 2-175
BAT-FAIL, page 2-41	LAN-POL-REV, page 2-114	RING-ID-MIS, page 2-176
BKUPMEMP, page 2-42	LASER-APR, page 2-115	RING-MISMATCH, page 2-176
BLSROSYNC, page 2-43	LASERBIAS-DEG, page 2-115	RING-SW-EAST, page 2-177
CARLOSS (CLIENT), page 2-43	LASERBIAS-FAIL, page 2-116	RING-SW-WEST, page 2-177
CARLOSS (EQPT), page 2-44	LASEREOL, page 2-116	RSVP-HELLODOWN, page 2-177
CARLOSS (E100T, E1000F), page 2-45	LASERTEMP-DEG, page 2-117	RUNCFG-SAVENEED, page 2-178
CARLOSS (G1000), page 2-46	LKOUTWK-S (NA), page 2-118	SD (CLIENT, TRUNK), page 2-178
CARLOSS (ML100T, ML1000), page 2-49	LKOUTPR-S, page 2-118	SD (DS1, DS3), page 2-178
CARLOSS (TRUNK), page 2-50	LMP-HELLODOWN, page 2-118	SD-L, page 2-180
CASETEMP-DEG, page 2-50	LMP-NDFAIL, page 2-118	SD-P, page 2-180
CKTDOWN, page 2-51	LOA, page 2-119	SF (CLIENT, TRUNK), page 2-181
CLDRESTART, page 2-53	LOCKOUT-REQ, page 2-119	SF (DS1, DS3), page 2-182
COMIOXC, page 2-54	LOF (BITS), page 2-120	SF-L, page 2-182
COMM-FAIL, page 2-54	LOF (CLIENT), page 2-121	SF-P, page 2-183
CONTBUS-A-18, page 2-55	LOF (DS1), page 2-121	SFTWDOWN, page 2-183
CONTBUS-B-18, page 2-55	LOF (DS3), page 2-122	SH-INS-LOSS-VAR-DEG-HIGH, page 2-183
CONTBUS-IO-A, page 2-56	LOF (EC1-12), page 2-123	SH-INS-LOSS-VAR-DEG-LOW, page 2-184
CONTBUS-IO-B, page 2-57	LOF (OCN), page 2-123	SHUTTER-OPEN, page 2-184
CTNEQPT-MISMATCH, page 2-58	LOF (TRUNK), page 2-124	SNTP-HOST, page 2-185
CTNEQPT-PBPROT, page 2-59	LOM, page 2-124	SPAN-SW-EAST, page 2-185
CTNEQPT-PBWORK, page 2-61	LOP-P, page 2-125	SPAN-SW-WEST, page 2-186
DATAFLT, page 2-62	LOP-V, page 2-125	SQUELCH, page 2-186
DBOSYNC, page 2-62	LO-RXPOWER, page 2-126	SQUELCHED, page 2-187
DSP-COMM-FAIL, page 2-63	LO-TXPOWER, page 2-137	SQM, page 2-188
DSP-FAIL, page 2-63	LOS (BITS), page 2-127	SSM-DUS, page 2-188
DS3-MISM, page 2-64	LOS (CLIENT), page 2-127	SSM-FAIL, page 2-189
DUP-IPADDR, page 2-65	LOS (DS1), page 2-128	SSM-LNC, page 2-189
DUP-NODENAME, page 2-65	LOS (DS3), page 2-129	SSM-OFF, page 2-189
EHIBATVG, page 2-66	LOS (EC1-12), page 2-130	SSM-PRC, page 2-190
ELWBATVG, page 2-66	LOS (FUDC), page 2-131	SSM-PRS, page 2-190
EOC, page 2-66	LOS (OCN), page 2-132	SSM-RES, page 2-190
EOC-L, page 2-68	LOS (OTS), page 2-134	SSM-SDH-TN, page 2-190

Table 2-6 Alphabetical Alarm Index (continued)

EQPT, page 2-69	LOS (TRUNK), page 2-135	SSM-SETS, page 2-191
EQPT-MISS, page 2-70	LOS-P, page 2-136	SSM-SMC, page 2-191
ERFI-P-CONN, page 2-71	LPBKCRS, page 2-138	SSM-ST2, page 2-191
ERFI-P-PAYLD, page 2-71	LPBKDS1FEAC, page 2-139	SSM-ST3, page 2-192
ERFI-P-SRVR, page 2-71	LPBKDS1FEAC-CMD, page 2-139	SSM-ST3E, page 2-192
ERROR-CONFIG, page 2-72	LPBKDS3FEAC, page 2-139	SSM-ST4, page 2-192
ETH-LINKLOSS, page 2-73	LPBKDS3FEAC-CMD, page 2-140	SSM-STU, page 2-191
E-W-MISMATCH, page 2-73	LPBKFACILITY (DS1, DS3), page 2-141	SSM-TNC, page 2-192
EXCCOL, page 2-75	LPBKFACILITY (CLIENT, TRUNK), page 2-140	SWMTXMOD, page 2-193
EXERCISE-RING-FAIL, page 2-76	LPBKFACILITY (EC1-12), page 2-141	SWTOPRI, page 2-194
EXERCISE-SPAN-FAIL, page 2-76	LPBKFACILITY (G1000), page 2-142	SWTOSEC, page 2-194
EXT, page 2-77	LPBKFACILITY (OCN), page 2-142	SWTOTHIRD, page 2-194
EXTRA-TRAF-PREEMPT, page 2-77	LPBKTERMINAL (CLIENT, TRUNK), page 2-143	SYNC-FREQ, page 2-195
FAILTOSW, page 2-78	LPBKTERMINAL (DS1, DS3, EC-1-12, OCN), page 2-144	SYNCPRI, page 2-195
FAILTOSW-PATH, page 2-79	LPBKTERMINAL (G1000), page 2-144	SYNCSEC, page 2-196
FAILTOSWR, page 2-79	LWBATVG, page 2-145	SYNCTHIRD, page 2-197
FAILTOSWS, page 2-81	MAN-REQ, page 2-145	SYSBOOT, page 2-197
FAN, page 2-83	MANRESET, page 2-146	TIM, page 2-198
FANDEGRADE, page 2-84	MANSWTOINT, page 2-146	TIM-MON, page 2-198
FE-AIS, page 2-84	MANSWTOPRI, page 2-146	TIM-P, page 2-199
FEC-MISM, page 2-84	MANSWTOSEC, page 2-146	TPTFAIL (FC_MR-4), page 2-200
FE-DS1-MULTLOS, page 2-85	MANSWTOTHIRD, page 2-147	TPTFAIL (G1000), page 2-200
FE-DS1-NSA, page 2-85	MANUAL-REQ-RING, page 2-147	TPTFAIL (ML100T, ML1000), page 2-201
FE-DS1-SA, page 2-86	MANUAL-REQ-SPAN, page 2-147	TRMT, page 2-201
FE-DS1-SNGLLOS, page 2-86	MEA (AIP), page 2-148	TRMT-MISS, page 2-202
FE-DS3-NSA, page 2-87	MEA (EQPT), page 2-148	TX-AIS, page 2-203
FE-DS3-SA, page 2-88	MEA (FAN), page 2-150	TX-RAI, page 2-203
FE-EQPT-NSA, page 2-88	MEM-GONE, page 2-151	UNC-WORD, page 2-203
FE-FRCDWKSWPR-RING, page 2-89	MEM-LOW, page 2-151	UNEQ-P, page 2-204
FE-FRCDWKSWPR-SPAN, page 2-89	MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151	UNEQ-V, page 2-206
FE-IDLE, page 2-90	NO-CONFIG, page 2-152	VCG-DEG, page 2-206

Table 2-6 Alphabetical Alarm Index (continued)

FE-LOCKOUTOFPR-SPAN, page 2-90	NOT-AUTHENTICATED, page 2-153	VCG-DOWN, page 2-207
FE-LOF, page 2-91	NTWTPINC, page 2-153	VOA-HDEG, page 2-207
FE-LOS, page 2-91	OCHNC-ACTIV-FAIL, page 2-153	VOA-HFAIL, page 2-208
FE-MANWKSWPR-RING, page 2-92	OCHNC-DEACTIV-FAIL, page 2-153	VOA-LDEG, page 2-208
FE-MANWKSWPR-SPAN, page 2-92	OCHNC-FAIL, page 2-153	VOA-LFAIL, page 2-209
FEPRLF, page 2-93	OCHNC-INC, page 2-153	WKSWPR, page 2-209
FORCED-REQ, page 2-94	ODUK-AIS-PM, page 2-154	WTR, page 2-210
FORCED-REQ-RING, page 2-94	ODUK-BDI-PM, page 2-154	WVL-MISMATCH, page 2-210
FORCED-REQ-SPAN, page 2-95	ODUK-LCK-PM, page 2-155	—

2.3 Logical Object Type Definitions

ONS 15454 alarms are grouped according to their logical object types in alarm profile listings (for example OCN::LOS). Each alarm entry in this chapter lists its type. These 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 Type/Object Definition

AICI-AEP	Alarm Interface Controller–International/Alarm Expansion Panel. A combination term that refers to this platform’s AIC card.
AICI-AIE	Alarm Interface Controller–International/Alarm Interface Extension. A combination term that refers to this platform’s AIC-I card.
AIP	Auxiliary interface protection module.
AOTS	Amplified optical transport section.
BITS	Building integration timing supply (BITS) incoming references (BITS-1, BITS-2).
BPLANE	The backplane.
CLIENT	The low-speed port, such as a transponder (TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G) or muxponder (MXP_2.5G_10G), where the optical signal is dropped.
DS1	A DS-1 line on a DS-1 card.
DS3	A DS-3 line on a DS-3 card.
EC1-12	An EC1-12 line on an EC1-12 card.
ENVALRM	An environmental alarm port.
EQPT	A card 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, STS, and VT.

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

EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2).
E100T	An E100 Ethernet card (E100T-12, E100T-G).
E1000F	An E1000 Ethernet card (E1000-2, E1000-2G).
FAN	Fan-tray assembly.
FCMR	An FC_MR-4 Fibre Channel card, not currently used in this release.
FUDC	SONET F1 byte user data channel.
G1000	A G1000 Ethernet card (G1000-4).
ML100T	An ML100 card (ML100T-12).
ML1000	An ML1000 Ethernet card (ML1000-2).
NE	The entire network element.
NE-SYNCH	Represents the timing status of the NE.
OCH	The optical channel, referring to dense wavelength division multiplexing (DWDM) cards.
OCN	An OC-N line on an OC-N card.
OMS	Optical multiplex section.
OTN	Optical transport network.
OSC-RING	Optical service channel ring.
PWR	Power.
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 dense wavelength division multiplexing (DWDM) card carrying the high-speed signal.
UCP-IPCC	Unified control plane (UCP) communication channel.
UCP-CKT	UCP circuit.
VCG	VT concatenation.
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 gives the name and page number of every alarm in the chapter, organized by logical object type.



Note

This alarm profile list is taken directly from the CTC interface. Some items do not appear in alphabetical order.

Table 2-8 Alarm Index by Alarm Type

AICI-AEP: EQPT, page 2-69	EQPT: MANRESET, page 2-146	OCN: SSM-STU, page 2-191
AICI-AEP: MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151	EQPT: MEA (EQPT), page 2-148	OCN: SSM-TNC, page 2-192
AICI-AIE: EQPT, page 2-69	MEM-GONE, page 2-151	OCN: SYNC-FREQ, page 2-195
AICI-AIE: MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151	EQPT:MEM-LOW, page 2-151	OCN: TIM, page 2-198
AIP: INVMACADR, page 2-111	EQPT: NO-CONFIG, page 2-152	OCN: WKSWPR, page 2-209
AIP: MEA (AIP), page 2-148	EQPT: PEER-NORESPONSE, page 2-166	OCN: WTR, page 2-210
AIP: MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151	EQPT: PROTNA, page 2-170	OMS: AS-CMD, page 2-32
AOTS: AMPLI-INIT, page 2-24	EQPT: PWR-REDUN, page 2-172	OMS: AS-MT, page 2-33
AOTS: AS-CMD, page 2-32	EQPT: RUNCFG-SAVENEED, page 2-178	OMS: OPWR-HDEG, page 2-158
AOTS: AS-MT, page 2-33	EQPT: SFTWDOWN, page 2-183	OMS: OPWR-HFAIL, page 2-160
AOTS: CASETEMP-DEG, page 2-50	EQPT: SWMTXMOD, page 2-193	OMS: OPWR-LDEG, page 2-160
AOTS: FIBERTEMP-DEG, page 2-94	EQPT: WKSWPR, page 2-209	OMS: OPWR-LFAIL, page 2-161
AOTS: GAIN-HDEG, page 2-97	EQPT: WTR, page 2-210	OMS: VOA-HDEG, page 2-207
AOTS: GAIN-HFAIL, page 2-98	EXT-SREF: FRCDSWTOPRI, page 2-95	OMS: VOA-HFAIL, page 2-208
AOTS: GAIN-LDEG, page 2-98	EXT-SREF: FRCDSWTOSEC, page 2-96	OMS: VOA-LDEG, page 2-208
AOTS: GAIN-LFAIL, page 2-99	EXT-SREF: FRCDSWTOHTRD, page 2-96	OMS: VOA-LFAIL, page 2-209
AOTS: LASER-APR, page 2-115	EXT-SREF: MANSWTOPRI, page 2-146	OSC-RING: NTWTPINC, page 2-153
AOTS: LASERBIAS-DEG, page 2-115	EXT-SREF: MANSWTOSEC, page 2-146	OSC-RING: RING-ID-MIS, page 2-176
AOTS: LASERBIAS-FAIL, page 2-116	EXT-SREF: MANSWTOHTRD, page 2-147	OTS: AS-CMD, page 2-32
AOTS: LASERTEMP-DEG, page 2-117	EXT-SREF: SWTOPRI, page 2-194	OTS: AS-MT, page 2-33
AOTS: OPWR-HDEG, page 2-158	EXT-SREF: SWTOSEC, page 2-194	OTS: AWG-DEG, page 2-40

Table 2-8 Alarm Index by Alarm Type (continued)

AOTS: OPWR-HFAIL, page 2-160	EXT-SREF: SWTOTHIRD, page 2-194	OTS: AWG-FAIL, page 2-40
AOTS: OPWR-LDEG, page 2-160	EXT-SREF: SYNCPRI, page 2-195	OTS: AWG-OVERTEMP, page 2-41
AOTS: OPWR-LFAIL, page 2-161	EXT-SREF: SYNCSEC, page 2-196	OTS: AWG-WARM-UP, page 2-41
AOTS: VOA-HDEG, page 2-207	EXT-SREF: SYNCTHIRD, page 2-197	OTS: LASERBIAS-DEG, page 2-115
AOTS: VOA-HFAIL, page 2-208	FAN: EQPT-MISS, page 2-70	OTS: LOS (OTS), page 2-134
AOTS: VOA-LDEG, page 2-208	FAN: FAN, page 2-83	OTS: OPWR-HDEG, page 2-158
AOTS: VOA-LFAIL, page 2-209	FAN: FANDEGRADE, page 2-84	OTS: OPWR-HFAIL, page 2-160
BITS: AIS, page 2-21	FAN: MEA (FAN), page 2-150	OTS: OPWR-LDEG, page 2-160
BITS: LOF (BITS), page 2-120	FAN: MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151	OTS: OPWR-LFAIL, page 2-161
BITS: LOS (BITS), page 2-127	FCMR: AS-CMD, page 2-32	OTS: SH-INS-LOSS-VAR-DEG-HIGH, page 2-183
BITS: SSM-DUS, page 2-188	FCMR: AS-MT, page 2-33	OTS: SH-INS-LOSS-VAR-DEG-LOW, page 2-184
BITS: SSM-FAIL, page 2-189	FCMR: INC-GFP-OUTOFFRAME, page 2-107	OTS: SHUTTER-OPEN, page 2-184
BITS: SSM-OFF, page 2-189	FCMR: INC-GFP-SIGLOSS, page 2-108	OTS: VOA-HDEG, page 2-207
BITS: SSM-PRS, page 2-190	FCMR: INC-GFP-SYNCLLOSS, page 2-108	OTS: VOA-HFAIL, page 2-208
BITS: SSM-RES, page 2-190	FCMR: INC-SIGLOSS, page 2-109	OTS: VOA-LDEG, page 2-208
BITS: SSM-SMC, page 2-191	FCMR: INC-SYNCLLOSS, page 2-110	OTS: VOA-LFAIL, page 2-209
BITS: SSM-ST2, page 2-191	FCMR: PORT-MISMATCH, page 2-169	PWR: AS-CMD, page 2-32
BITS: SSM-ST3, page 2-192	FCMR: TPTFAIL (FC_MR-4), page 2-200	PWR: BAT-FAIL, page 2-41
BITS: SSM-ST3E, page 2-192	FUDC: AIS, page 2-21	PWR: EHIBATVG, page 2-66
BITS: SSM-ST4, page 2-192	FUDC: LOS (FUDC), page 2-131	PWR: ELWBATVG, page 2-66
BITS: SSM-STU, page 2-191	G1000: AS-CMD, page 2-32	PWR: HIBATVG, page 2-100
BITS: SSM-TNC, page 2-192	G1000: AS-MT, page 2-33	PWR: LWBATVG, page 2-145

Table 2-8 Alarm Index by Alarm Type (continued)

BITS: SYNC-FREQ, page 2-195	G1000: CARLOSS (G1000), page 2-46	STSMON: AIS-P, page 2-22
BPLANE: AS-CMD, page 2-32	G1000: LPBKFACILITY (G1000), page 2-142	STSMON: AUTOSW-AIS, page 2-36
BPLANE: MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN), page 2-151	G1000: LPBKTERMINAL (G1000), page 2-144	STSMON: AUTOSW-LOP (STSMON), page 2-37
CLIENT: AIS, page 2-21	G1000: TPTFAIL (G1000), page 2-200	STSMON: AUTOSW-PDI, page 2-38
CLIENT: ALS, page 2-23	ML1000: AS-CMD, page 2-32	STSMON: AUTOSW-SDBER, page 2-38
CLIENT: AS-CMD, page 2-32	ML1000: CARLOSS (ML100T, ML1000), page 2-49	STSMON: AUTOSW-SFBER, page 2-38
CLIENT: AS-MT, page 2-33	ML1000: TPTFAIL (ML100T, ML1000), page 2-201	STSMON: AUTOSW-UNEQ (STSMON), page 2-39
CLIENT: CARLOSS (CLIENT), page 2-43	ML100T: AS-CMD, page 2-32	STSMON: ERFI-P-CONN, page 2-71
CLIENT: EOC, page 2-66	ML100T: CARLOSS (ML100T, ML1000), page 2-49	STSMON: ERFI-P-PAYLD, page 2-71
CLIENT: EOC-L, page 2-68	ML100T: TPTFAIL (ML100T, ML1000), page 2-201	STSMON: ERFI-P-SRVR, page 2-71
CLIENT: FAILTOSW, page 2-78	MSUDC: AIS, page 2-21	STSMON: FAILTOSW-PATH, page 2-79
CLIENT: FORCED-REQ-SPAN, page 2-95	MSUDC: LOS (MSUDC), page 2-132	STSMON: FORCED-REQ, page 2-94
CLIENT: GE-OOSYNC, page 2-100	NE-SREF: FRCDSWTOINT, page 2-95	STSMON: LOCKOUT-REQ, page 2-119
CLIENT: HI-LASERBIAS, page 2-101	NE-SREF: FRCDSWTOPRI, page 2-95	STSMON: LOP-P, page 2-125
CLIENT: HI-RXPOWER, page 2-102	NE-SREF: FRCDSWTOSEC, page 2-96	STSMON: LPBKCRS, page 2-138
CLIENT: HI-TXPOWER, page 2-103	NE-SREF: FRCDSWTOTHIRD, page 2-96	STSMON: MAN-REQ, page 2-145
CLIENT: LO-RXPOWER, page 2-126	NE-SREF: FRNGSYNC, page 2-96	STSMON: PDI-P, page 2-164
CLIENT: LO-TXPOWER, page 2-137	NE-SREF: FSTSYNC, page 2-97	STSMON: PLM-P, page 2-167
CLIENT: LOCKOUT-REQ, page 2-119	NE-SREF: HLDVRSYNC, page 2-104	STSMON: RFI-P, page 2-174
CLIENT: LOF (CLIENT), page 2-121	NE-SREF: MANSWTOINT, page 2-146	STSMON: SD-P, page 2-180

Table 2-8 Alarm Index by Alarm Type (continued)

CLIENT: LOS (CLIENT), page 2-127	NE-SREF: MANSWTOPRI, page 2-146	STSMON: SF-P, page 2-183
CLIENT: LPBKFACILITY (CLIENT, TRUNK), page 2-140	NE-SREF: MANSWTOSEC, page 2-146	STSMON: TIM-P, page 2-199
CLIENT: LPBKTERMINAL (CLIENT, TRUNK), page 2-143	NE-SREF: MANSWTO THIRD, page 2-147	STSMON: UNEQ-P, page 2-204
CLIENT: MANUAL-REQ-SPAN, page 2-147	NE-SREF: SSM-PRS, page 2-190	STSMON: WKS WPR, page 2-209
CLIENT: OUT-OF-SYNC, page 2-164	NE-SREF: SSM-RES, page 2-190	STSMON: WTR, page 2-210
CLIENT: PORT-CODE-MISM, page 2-168	NE-SREF: SSM-SMC, page 2-191	STSTRM: AIS-P, page 2-22
CLIENT: PORT-COMM-FAIL, page 2-168	NE-SREF: SSM-ST2, page 2-191	STSTRM: AU-LOF, page 2-34
CLIENT: PORT-MISMATCH, page 2-169	NE-SREF: SSM-ST3, page 2-192	STSTRM: ERFI-P-CONN, page 2-71
CLIENT: PORT-MISSING, page 2-169	NE-SREF: SSM-ST3E, page 2-192	STSTRM: ERFI-P-PAYLD, page 2-71
CLIENT: RFI, page 2-173	NE-SREF: SSM-ST4, page 2-192	STSTRM: ERFI-P-SRVR, page 2-71
CLIENT: SD (CLIENT, TRUNK), page 2-178	NE-SREF: SSM-STU, page 2-191	STSTRM: LOM, page 2-124
CLIENT: SF (CLIENT, TRUNK), page 2-181	NE-SREF: SSM-TNC, page 2-192	STSTRM: LOP-P, page 2-125
CLIENT: SQUELCHED, page 2-187	NE-SREF: SWTOPRI, page 2-194	STSTRM: OOU-TPT, page 2-157
CLIENT: SSM-DUS, page 2-188	NE-SREF: SWTOSEC, page 2-194	STSTRM: PDI-P, page 2-164
CLIENT: SSM-FAIL, page 2-189	NE-SREF: SWTO THIRD, page 2-194	STSTRM: PLM-P, page 2-167
CLIENT: SSM-LNC, page 2-189	NE-SREF: SYNCPRI, page 2-195	STSTRM: RFI-P, page 2-174
CLIENT: SSM-OFF, page 2-189	NE-SREF: SYNCSEC, page 2-196	STSTRM: SD-P, page 2-180
CLIENT: SSM-PRC, page 2-190	NE-SREF: SYNCTHIRD, page 2-197	STSTRM: SF-P, page 2-183
CLIENT: SSM-PRS, page 2-190	NE: APC-DISABLED, page 2-24	STSTRM: SQM, page 2-188
CLIENT: SSM-RES, page 2-190	NE: APC-FAIL, page 2-25	STSTRM: TIM-P, page 2-199
CLIENT: SSM-SDH-TN, page 2-190	NE: AS-CMD, page 2-32	STSTRM: UNEQ-P, page 2-204

Table 2-8 Alarm Index by Alarm Type (continued)

CLIENT: SSM-SETS, page 2-191	NE: AUD-LOG-LOSS, page 2-34	TRUNK: AIS, page 2-21
CLIENT: SSM-SMC, page 2-191	NE: AUD-LOG-LOW, page 2-34	TRUNK: ALS, page 2-23
CLIENT: SSM-ST2, page 2-191	NE: DATAFLT, page 2-62	TRUNK: AS-CMD, page 2-32
CLIENT: SSM-ST3, page 2-192	NE: DBOSYNC, page 2-62	TRUNK: AS-MT, page 2-33
CLIENT: SSM-ST3E, page 2-192	NE: DUP-IPADDR, page 2-65	TRUNK: CARLOSS (TRUNK), page 2-50
CLIENT: SSM-ST4, page 2-192	NE: DUP-NODENAME, page 2-65	TRUNK: DSP-COMM-FAIL, page 2-63
CLIENT: SSM-STU, page 2-191	NE: ETH-LINKLOSS, page 2-73	TRUNK: DSP-FAIL, page 2-63
CLIENT: SSM-TNC, page 2-192	NE: HITEMP, page 2-103	TRUNK: EOC, page 2-66
CLIENT: SYNC-FREQ, page 2-195	NE: I-HITEMP, page 2-105	TRUNK: EOC-L, page 2-68
CLIENT: TIM, page 2-198	NE: INTRUSION-PSWD, page 2-111	TRUNK: FAILTOSW, page 2-78
CLIENT: TIM-MON, page 2-198	NE: LAN-POL-REV, page 2-114	TRUNK: FEC-MISM, page 2-84
CLIENT: WKSWPR, page 2-209	NE: OPTNTWMIS, page 2-157	TRUNK: FORCED-REQ-SPAN, page 2-95
CLIENT: WTR, page 2-210	NE: SNTP-HOST, page 2-185	TRUNK: GCC-EOC, page 2-100
DS1: AIS, page 2-21	NE: SYSBOOT, page 2-197	TRUNK: GE-OOSYNC, page 2-100
DS1: AS-CMD, page 2-32	OCH: AS-CMD, page 2-32	TRUNK: HI-LASERBIAS, page 2-101
DS1: AS-MT, page 2-33	OCH: AS-MT, page 2-33	TRUNK: HI-RXPOWER, page 2-102
DS1: LOF (DS1), page 2-121	OCH: OPWR-HDEG, page 2-158	TRUNK: HI-TXPOWER, page 2-103
DS1: LOS (DS1), page 2-128	OCH: OPWR-HFAIL, page 2-160	TRUNK: LO-RXPOWER, page 2-126
DS1: LPBKDS1FEAC, page 2-139	OCH: OPWR-LDEG, page 2-160	TRUNK: LO-TXPOWER, page 2-137
DS1: LPBKDS1FEAC-CMD, page 2-139	OCH: OPWR-LFAIL, page 2-161	TRUNK: LOCKOUT-REQ, page 2-119
DS1: LPBKFACILITY (DS1, DS3), page 2-141	OCH: VOA-HDEG, page 2-207	TRUNK: LOF (TRUNK), page 2-124
DS1: LPBKTERMINAL (DS1, DS3, EC-1-12, OCN), page 2-144	OCH: VOA-HFAIL, page 2-208	TRUNK: LOM, page 2-124
DS1: RAI, page 2-172	OCH: VOA-LDEG, page 2-208	TRUNK: LOS (TRUNK), page 2-135

Table 2-8 Alarm Index by Alarm Type (continued)

DS1: RCVR-MISS, page 2-173	OCH: VOA-LFAIL, page 2-209	TRUNK: LOS-P, page 2-136
DS1: SD (DS1, DS3), page 2-178	OCHNC-CONN: OCHNC-ACTIV-FAIL, page 2-153	TRUNK: LPBKFACILITY (CLIENT, TRUNK), page 2-140
DS1: SF (DS1, DS3), page 2-182	OCHNC-CONN: OCHNC-DEACTIV-FAIL, page 2-153	TRUNK: LPBKTERMINAL (CLIENT, TRUNK), page 2-143
DS1: TRMT, page 2-201	OCHNC-CONN: OCHNC-FAIL, page 2-153	TRUNK: MANUAL-REQ-SPAN, page 2-147
DS1: TRMT-MISS, page 2-202	OCHNC-CONN: OCHNC-INC, page 2-153	TRUNK: ODUK-AIS-PM, page 2-154
DS1: TX-AIS, page 2-203	OCN: AIS-L, page 2-22	TRUNK: ODUK-BDI-PM, page 2-154
DS1: TX-RAI, page 2-203	OCN: ALS, page 2-23	TRUNK: ODUK-LCK-PM, page 2-155
DS3: AIS, page 2-21	OCN: APSB, page 2-26	TRUNK: ODUK-OCI-PM, page 2-155
DS3: AS-CMD, page 2-32	OCN: APSC-IMP, page 2-27	TRUNK: ODUK-SD-PM, page 2-156
DS3: AS-MT, page 2-33	OCN: APSCDFLTK, page 2-27	TRUNK: ODUK-SF-PM, page 2-156
DS3: DS3-MISM, page 2-64	OCN: APSCINCON, page 2-29	TRUNK: ODUK-TIM-PM, page 2-156
DS3: FE-AIS, page 2-84	OCN: APSCM, page 2-29	TRUNK: OTUK-AIS, page 2-161
DS3: FE-DS1-MULTLOS, page 2-85	OCN: APSCNMIS, page 2-30	TRUNK: OTUK-BDI, page 2-162
DS3: FE-DS1-NSA, page 2-85	OCN: APSIMP, page 2-31	TRUNK: OTUK-LOF, page 2-162
DS3: FE-DS1-SA, page 2-86	OCN: APSMM, page 2-32	TRUNK: OTUK-SD, page 2-163
DS3: FE-DS1-SNGLLOS, page 2-86	OCN: AS-CMD, page 2-32	TRUNK: OTUK-LOF, page 2-162
DS3: FE-DS3-NSA, page 2-87	OCN: AS-MT, page 2-33	TRUNK: OTUK-TIM, page 2-164
DS3: FE-DS3-SA, page 2-88	OCN: AUTOLSROFF, page 2-35	TRUNK: OUT-OF-SYNC, page 2-164
DS3: FE-EQPT-NSA, page 2-88	OCN: BLSROSYNC, page 2-43	TRUNK: PTIM, page 2-171
DS3: FE-IDLE, page 2-90	OCN: E-W-MISMATCH, page 2-73	TRUNK: RFI, page 2-173
DS3: FE-LOF, page 2-91	OCN: EOC, page 2-66	TRUNK: SD (CLIENT, TRUNK), page 2-178

Table 2-8 Alarm Index by Alarm Type (continued)

DS3: FE-LOS, page 2-91	OCN: EOC-L, page 2-68	TRUNK: SF (DS1, DS3), page 2-182
DS3: INC-ISD, page 2-109	OCN: EXERCISE-RING-FAIL, page 2-76	TRUNK: SSM-DUS, page 2-188
DS3: LOF (DS3), page 2-122	OCN: EXERCISE-SPAN-FAIL, page 2-76	TRUNK: SSM-FAIL, page 2-189
DS3: LOS (DS3), page 2-129	OCN: EXTRA-TRAF-PREEMPT, page 2-77	TRUNK: SSM-LNC, page 2-189
DS3: LPBKDS1FEAC, page 2-139	OCN: FAILTOSW, page 2-78	TRUNK: SSM-OFF, page 2-189
DS3: LPBKDS3FEAC, page 2-139	OCN: FAILTOSWR, page 2-79	TRUNK: SSM-PRC, page 2-190
DS3: LPBKDS3FEAC-CMD, page 2-140	OCN: FAILTOSWS, page 2-81	TRUNK: SSM-PRS, page 2-190
DS3: LPBKFACILITY (DS1, DS3), page 2-141	OCN: FE-FRCDWKSWPR-RING, page 2-89	TRUNK: SSM-RES, page 2-190
DS3: LPBKTERMINAL (DS1, DS3, EC-1-12, OCN), page 2-144	OCN: FE-FRCDWKSWPR-SPAN, page 2-89	TRUNK: SSM-SDH-TN, page 2-190
DS3: RAI, page 2-172	OCN: FE-LOCKOUTOFPR-SPAN, page 2-90	TRUNK: SSM-SETS, page 2-191
DS3: SD (DS1, DS3), page 2-178	OCN: FE-MANWKSWPR-RING, page 2-92	TRUNK: SSM-SMC, page 2-191
DS3: SF (DS1, DS3), page 2-182	OCN: FE-MANWKSWPR-SPAN, page 2-92	TRUNK: SSM-ST2, page 2-191
E1000F: AS-CMD, page 2-32	OCN: FEPRLF, page 2-93	TRUNK: SSM-ST3, page 2-192
E1000F: CARLOSS (E100T, E1000F), page 2-45	OCN: FORCED-REQ-RING, page 2-94	TRUNK: SSM-ST3E, page 2-192
E100T: AS-CMD, page 2-32	OCN: FORCED-REQ-SPAN, page 2-95	TRUNK: SSM-ST4, page 2-192
E100T: CARLOSS (E100T, E1000F), page 2-45	OCN: FULLPASSTHR-BI, page 2-97	TRUNK: SSM-STU, page 2-191
EC1-12: AIS-L, page 2-22	OCN: HI-LASERBIAS, page 2-101	TRUNK: SSM-TNC, page 2-192
EC1-12: AS-CMD, page 2-32	OCN: HI-RXPOWER, page 2-102	TRUNK: SYNC-FREQ, page 2-195
EC1-12: AS-MT, page 2-33	OCN: HI-TXPOWER, page 2-103	TRUNK: TIM, page 2-198

Table 2-8 Alarm Index by Alarm Type (continued)

EC1-12: LOF (EC1-12), page 2-123	OCN: KB-PASSTHR, page 2-114	TRUNK: TIM-MON, page 2-198
EC1-12: LOS (EC1-12), page 2-130	OCN: KBYTE-APS-CHANNEL-FAILURE, page 2-114	TRUNK: UNC-WORD, page 2-203
EC1-12: LPBKFACILITY (EC1-12), page 2-141	OCN: LASEREOL, page 2-116	TRUNK: WKSWPR, page 2-209
EC1-12: LPBKFACILITY (EC1-12), page 2-141	OCN: LKOUTPR-S, page 2-118	TRUNK: WTR, page 2-210
EC1-12: RFI-L, page 2-174	OCN: LO-RXPOWER, page 2-126	TRUNK: WVLMISMATCH, page 2-210
EC1-12: SD-L, page 2-180	OCN: LO-TXPOWER, page 2-137	UCP-CKT: CKTDOWN, page 2-51
EC1-12: SF-L, page 2-182	OCN: LOCKOUT-REQ, page 2-119	UCP-IPCC: LMPHELLODOWN, page 2-118
ENVALRM: EXT, page 2-77	OCN: LOF (OCN), page 2-123	UCP-IPCC: LMPNDFAIL, page 2-118
EQPT: AS-CMD, page 2-32	OCN: LOS (OCN), page 2-132	UCP-NBR: RSVPHELLODOWN, page 2-177
EQPT: AUTORESET, page 2-36	OCN: LPBKFACILITY (OCN), page 2-142	VCG: LOA, page 2-119
EQPT: BKUPMEMP, page 2-42	OCN: LPBKTERMINAL (DS1, DS3, EC-1-12, OCN), page 2-144	VCG: VCG-DEG, page 2-206
EQPT: CARLOSS (EQPT), page 2-44	OCN: MANUAL-REQ-RING, page 2-147	VCG: VCG-DOWN, page 2-207
EQPT: CLDRESTART, page 2-53	OCN: MANUAL-REQ-SPAN, page 2-147	VT-MON: AIS-V, page 2-23
EQPT: COMIOXC, page 2-54	OCN: PRC-DUPID, page 2-170	VT-MON: AUTOSW-AIS, page 2-36
EQPT: COMM-FAIL, page 2-54	OCN: RFI-L, page 2-174	VT-MON: AUTOSW-LOP (VT-MON), page 2-37
EQPT: CONTBUS-A-18, page 2-55	OCN: RING-ID-MIS, page 2-176	VT-MON: AUTOSW-UNEQ (VT-MON), page 2-39
EQPT: CONTBUS-B-18, page 2-55	OCN: RING-MISMATCH, page 2-176	VT-MON: FAILTOSW-PATH, page 2-79
EQPT: CONTBUS-IO-A, page 2-56	OCN: RING-SW-EAST, page 2-177	VT-MON: FORCED-REQ, page 2-94
EQPT: CONTBUS-IO-B, page 2-57	OCN: RING-SW-WEST, page 2-177	VT-MON: LOCKOUT-REQ, page 2-119
EQPT: CTNEQPT-MISMATCH, page 2-58	OCN: SD-L, page 2-180	VT-MON: LOP-V, page 2-125

Table 2-8 Alarm Index by Alarm Type (continued)

EQPT: CTNEQPT-PBPROT , page 2-59	OCN: SF-L , page 2-182	VT-MON: MAN-REQ , page 2-145
EQPT: CTNEQPT-PBWORK , page 2-61	OCN: SPAN-SW-EAST , page 2-185	VT-MON: UNEQ-V , page 2-206
EQPT: EQPT , page 2-69	OCN: SPAN-SW-WEST , page 2-186	VT-MON: WKSWPR , page 2-209
EQPT: ERROR-CONFIG , page 2-72	OCN: SQUELCH , page 2-186	VT-MON: WTR , page 2-210
EQPT: EXCCOL , page 2-75	OCN: SSM-DUS , page 2-188	VT-TERM: AIS-V , page 2-23
EQPT: FAILTOSW , page 2-78	OCN: SSM-FAIL , page 2-189	VT-TERM: LOM , page 2-124
EQPT: FORCED-REQ , page 2-94	OCN: SSM-OFF , page 2-189	VT-TERM: LOP-V , page 2-125
EQPT: HITEMP , page 2-103	OCN: SSM-PRS , page 2-190	VT-TERM: OOU-TPT , page 2-157
EQPT: IMPROPRMVL , page 2-105	OCN: SSM-RES , page 2-190	VT-TERM: PLM-V , page 2-167
EQPT: INHSWPR , page 2-110	OCN: SSM-SMC , page 2-191	VT-TERM: RFI-V , page 2-175
EQPT: INHSWWKG , page 2-110	OCN: SSM-ST2 , page 2-191	VT-TERM: SD-P , page 2-180
EQPT: IOSCFGCOPY , page 2-113	OCN: SSM-ST3 , page 2-192	VT-TERM: SF-P , page 2-183
EQPT: LOCKOUT-REQ , page 2-119	OCN: SSM-ST3E , page 2-192	VT-TERM: SQM , page 2-188
EQPT: MAN-REQ , page 2-145	OCN: SSM-ST4 , page 2-192	VT-TERM: UNEQ-V , page 2-206

2.5 Trouble Notifications

The ONS 15454 uses standard Telcordia categories to characterize levels of trouble. The ONS 15454 reports alarmed trouble notifications and Not-Alarmed (NA) notifications, if selected, in the CTC Alarms window. Alarms typically signify a problem that the user needs to fix, such as a loss of signal (LOS), while Not-Alarmed (NA) notifications do not necessarily need immediate troubleshooting.

Telcordia further divides alarms into Service-Affecting (SA) and NSA status. A Service-Affecting (SA) failure affects a provided service or the network's ability to provide service. For example, the [“TRMT-MISS” alarm on page 2-202](#) is characterized by default as an SA failure. TRMT-MISS occurs when a cable connector is removed from an active DS-1 card port. The default severity assumes that service has been interrupted or moved. If the DS-1 card is in a protection group and the traffic is on the protect card rather than the working card, or if the port with the TRMT-MISS alarm has no circuits provisioned, TRMT-MISS would be raised as NSA because traffic was not interrupted or moved.

2.5.1 Conditions

The term “Condition” refers to any problem detected on an ONS 15454 shelf whether or not the problem is reported (that is, whether or not it generates a trouble notification). Reported conditions include alarms, Not-Alarmed conditions, and Not-Reported (NR) conditions. A snapshot of all current raised conditions on a node, whether they are reported or not, can be retrieved using the CTC Conditions window or using TLI’s set of RTRV-COND commands. You can see the actual reporting messages for alarms and NAs in the CTC History tab.

For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 and Cisco ONS 15327 TLI Command Guide*.

2.5.2 Severities

The ONS 15454 uses Telcordia standard severities: Critical (CR), Major (MJ), and Minor (MN). Non-Service Affecting (NSA) alarms always have a Minor (MN) severity. Service-Affecting (SA) alarms can be Critical (CR), Major (MJ), or Minor (MN). Critical alarms generally indicate severe, service-affecting trouble that needs immediate correction. A Major (MJ) alarm is a serious alarm, but the trouble has less impact on the network. For SONET signal alarms, loss of traffic on more than five DS-1 circuits is Critical. Loss of traffic on one to five DS-1 circuits is Major (MJ). Loss of traffic on an STS-1, which can hold 28 DS-1 circuits, would be a Critical (CR), Service-Affecting (SA) alarm.

An example of a Non-Service Affecting (NSA) alarm is the “[FSTSYNC](#)” condition on page 2-97 (Fast Start Synchronization Mode), which indicates the ONS 15454 is choosing a new timing reference because the previously used reference has failed. The user needs to troubleshoot the loss of the prior timing source, but the loss is not immediately disruptive to service.

Telcordia standard severities are the default settings for the ONS 15454. A user can customize ONS 15454 alarm severities with the alarm profiles feature. For alarm profile procedures, refer to the *Cisco ONS 15454 Procedure Guide*.

This chapter lists the default profile alarm severity for the Service-Affecting (SA) case of each alarm when it is applicable. Any alarm with a profile value of Critical (CR) or Major (MJ) will, if reported as Non-Service Affecting (NSA) because no traffic is lost, be reported with a Minor (MN) severity instead, in accordance with Telcordia rules.

2.6 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 warnings.

**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 (IS) for the laser to be on. The laser is off when the safety key is off (labeled 0).

**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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.

**Warning**

Class 1 laser product.

**Warning**

Class 1M laser radiation when open. Do not view directly with optical instruments.

2.7 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, 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*.

**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*.

2.7.1 AIS

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

**Note**

The MSUDC object is not supported in this platform in this release. It is reserved for future development.

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 tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The fault condition AIS 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**

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 2-132, or out-of-service (OOS) ports.
- Step 2** Clear the upstream alarms using the applicable procedures in this chapter.
- 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).
-

2.7.2 AIS-L

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

The AIS Line (AIS-L) condition indicates that this node is detecting line-level AIS in the incoming signal.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The fault condition AIS is raised by the receiving node on each input when it sees the signal 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 2-22.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.3 AIS-P

- Not Reported (NR), Non-Service Affecting (NSA)

- Logical Objects: STSMON, STSTRM

The AIS Path (AIS-P) condition means that this node is detecting AIS in the incoming path.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The fault condition AIS is raised by the receiving node on each input when it sees the signal 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 2-22.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.4 AIS-V

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

The AIS Virtual Tributary (VT) condition (AIS-V) means that this node is detecting AIS in the incoming VT-level path.

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The fault condition AIS is raised by the receiving node on each input when it sees the signal 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 “[AIS-V on DS3XM-6 Unused VT Circuits](#)” section on page 1-89 for more information.

Clear the AIS-V Condition

-
- Step 1** Complete the “[Clear the AIS Condition](#)” procedure on page 2-22.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.5 ALS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The Automatic Laser Shutdown (ALS) condition occurs when a DWDM amplifier (OPT-BST or OPT-PRE) 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. It does not require troubleshooting.

2.7.6 AMPLI-INIT

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Amplifier Initialized (AMPLI-INIT) condition occurs when a DWDM amplifier card (OPT-BST or OPT-PRE) is not able to calculate gain. This condition is typically raised with the [“APC-DISABLED” alarm on page 2-24](#).

Clear the AMPLI-INIT Condition

-
- Step 1** Complete the [“Delete a Circuit” procedure on page 2-217](#) 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/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.7 APC-DISABLED

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The Automatic Power Control (APC) Disabled (APC-DISABLED) alarm occurs when the information related to the number of channels is not reliable. The alarm can occur when the any of the following alarms also occur: the [“EQPT” alarm on page 2-69](#), the [“IMPROPRMVL” alarm on page 2-105](#), or the [“MEA \(EQPT\)” alarm on page 2-148](#). If the alarm occurs with the creation of the first circuit, delete and recreate it.

Clear the APC-DISABLED Alarm

-
- Step 1** Complete the appropriate procedure to clear the main alarm:
- [Clear the EQPT Alarm, page 2-70](#)
 - [Clear the IMPROPRMVL Alarm, page 2-106](#)
 - [Clear the MEA \(EQPT\) Alarm, page 2-148](#)
- Step 2** If the alarm does not clear, complete the [“Delete a Circuit” procedure on page 2-217](#) and then recreate it.

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

2.7.8 APC-FAIL

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The APC Failure (APC-FAIL) alarm occurs when APC has not been able to create a setpoint on a node because it has exceeded all allocated power margins including gain, power, or attenuation. These power margins (from 0 dB to 3 dB) are allocated when the network is installed. Margins can be consumed due to fiber aging or the insertion of unexpected extra loss in the span after a fiber cut.

Clear the APC-FAIL Alarm

- Step 1** Determine whether the increased margin use is due to fiber aging:
- a. Complete the task for checking OSC span attenuation in the *Cisco ONS 15454 Procedure Guide* Chapter 7, “Turn Up DWDM Network.”
 - b. Obtain the original MetroPlanner *.cmn file, then cross-reference original span values with current ones (obtained in CTC) to determine whether a loss of 0 dB to 3dB or more has occurred across the questioned span. To obtain current values, complete the procedure for verifying optical receive power in the *Cisco ONS 15454 Procedure Guide* Chapter 7, “Turn Up DWDM Network.”
 - c. On the degraded span, test fiber integrity by using optical testing equipment to verify port levels. Then verify these levels against each termination listed in CTC. To do this, complete the task for verifying DWDM card parameters in the *Cisco ONS 15454 Procedure Guide* Chapter 7, “Turn Up DWDM Network.”



Note Throughout this trouble isolation process, ensure that safe and proper fiber cleaning and scoping procedures are used. Follow established site practices or, if none exists, complete the procedure for cleaning fiber connectors in the *Cisco ONS 15454 Procedure Guide* Chapter 17, “Maintain the Node.”

- Step 2** If the span problem is due to aged fiber, replace it by completing the task to install fiber optic cables on DWDM cards in the *Cisco ONS 15454 Procedure Guide* Chapter 2, “Install Cards and Fiber-Optic Cable.”

- Step 3** If the trouble is not due to aging but to a fiber cut:
- a. Verify the alarms by completing the procedure for viewing alarms, history, events and conditions in the *Cisco ONS 15454 Procedure Guide* Chapter 9, “Manage Alarms.”
 - b. Complete the procedures in the “[Identify Points of Failure on an Optical Circuit Path](#)” section on [page 1-37](#).
 - c. Resolve the issue and alarm by completing the procedure to verify the optical receive power in the *Cisco ONS 15454 Procedure Guide* Chapter 7, “Turn Up DWDM Network.”
 - d. If the LOS alarm is raised against a relevant OCN object, complete the “[Clear the LOS \(OCN\) Alarm](#)” procedure on [page 2-133](#).

- 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).
-

2.7.9 APSB

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

The Automatic Protection Switching (APS) Channel Byte Failure (APSB) alarm occurs when line terminating equipment detects protection switching byte failure or an invalid 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 causes an APSB on an ONS node.

Clear the APSB Alarm

- 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 may 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 may need to replace the upstream cards for protection switching to operate properly. Complete the [“Physically Replace a Card” procedure on page 2-219](#).



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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.



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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.10 APSC-IMP

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

An Improper APS Code (APSC-IMP) alarm indicates bad or invalid K bytes. APSC-IMP occurs on OC-N cards in an MS-SPRing configuration. The receiving equipment monitors K bytes or K1 and K2 APS bytes for an indication to switch from the working card to the protect card or vice versa. K1/K2 bytes also contain bits that tell the receiving equipment whether the K byte is valid. The alarm clears when the node receives valid K bytes.

**Caution**

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

**Note**

This alarm can occur when the exercise command or a Lock Out is applied to a span. An externally switched span does not raise this alarm because traffic is preempted.

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.
- 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, complete the [“Identify a BLSR Ring Name or Node ID Number” procedure on page 2-213](#).
- Step 3** Repeat [Step 2](#) for all nodes in the ring.
- Step 4** If a node has a ring name number that does not match the other nodes, complete the [“Change a BLSR Ring Name” procedure on page 2-213](#) to make the ring names identical.
- Step 5** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.11 APSCDFLTK

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

The APS Default K Byte Received (APSCDFLTK) alarm occurs when a bidirectional line switched ring (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 2-43.

Clear the APSCDFLTK Alarm

-
- Step 1** Complete the “[Identify a BLSR Ring Name or Node ID Number](#)” procedure on page 2-213 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 2-214 to change one node’s 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 2-73.) West port fibers must connect to east port fibers, and vice versa. The *Cisco ONS 15454 Procedure Guide* provides a procedure for fibering BLSRs.
- Step 5** If the alarm does not clear and if 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 protection fiber.
- Step 6** If the alarm does not clear, complete the “[Verify Node Visibility for Other Nodes](#)” procedure on page 2-214.
- Step 7** If nodes are not visible, complete the “[Verify or Create Node DCC Terminations](#)” procedure on page 2-214 to ensure that SONET data communications channel (DCC) terminations exist on each node.
- Step 8** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.12 APSC-IMP

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

An Improper SONET APS Code (APSC-IMP) alarm indicates bad or invalid K bytes. The APSC-IMP alarm occurs on OC-N cards in a BLSR configuration. The receiving equipment monitors K bytes or K1 and K2 APS bytes for an indication to switch from the working card to the protect card or vice versa. K1/K2 bytes also contain bits that tell the receiving equipment whether the K byte is valid. The alarm clears when the node receives valid K bytes.



Caution

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



Note

This alarm can occur on a virtual tributary (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.

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.
- 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 2-213.
- 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 the ring name of that node identical to the other nodes. Complete the “[Change a BLSR Ring Name](#)” procedure on page 2-213.
- Step 5** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.13 APSCINCON

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

An APS Inconsistent (APSCINCON) 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 2-132, the “[LOF \(OCN\)](#)” alarm on page 2-123, or the “[AIS](#)” alarm on page 2-21. Clearing these alarms clears the APSCINCON alarm.
- Step 2** If an APSCINCON alarm occurs with no other alarms, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.14 APSCM

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

The APS Channel Mismatch (APSCM) alarm occurs when the ONS 15454 expects a working channel but receives a protection channel. In many cases, the working and protection 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 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 (IS) for the laser to be on. The laser is off when the safety key is off (labeled 0).

**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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.

**Caution**

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

Clear the APSCM Alarm

-
- Step 1** Verify that the working-card channel fibers are physically connected directly to the adjoining node's working-card channel fibers.
 - Step 2** If the fibers are correctly connected, verify that the protection-card channel fibers are physically connected directly to the adjoining node's protection-card channel fibers.
 - Step 3** 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.
-

2.7.15 APSCNMIS

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

The APS Node ID Mismatch (APSCNMIS) alarm occurs when the source node ID contained in the SONET K2 byte of the incoming APS channel 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 2-213](#) 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 2-214 to change one node’s 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 15454 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 “[Lock Out a BLSR Span](#)” procedure on page 2-215 to lock out the span.
- Step 6** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-215 to clear the lockout.
- Step 7** 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.

2.7.16 APSIMP

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

The APS Invalid Code (APSIMP) 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 proper type of byte.

The condition is superseded by an APS, APSCM, or APSMM. It is not superseded by AIS or 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 far end is not configured for 1+1 protection, create the group.
- 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.17 APSMM

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

An APS Mode Mismatch (APSMM) failure alarm occurs when there is a mismatch of the protection switching schemes at the two ends of the span. If one node is provisioned for bidirectional switching, the node at the other end of the span must also be provisioned for bidirectional switching. If one end is provisioned for bidirectional and the other is provisioned for unidirectional, an APSMM alarm occurs in the ONS node that is provisioned for bidirectional. The APSMM alarm occurs in a 1+1 configuration.

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 DCC connectivity) to the far end.
Click **Edit**.
Record whether the Bidirectional Switching check box is checked.
- Step 2** Log into the far-end node and verify that the OC-N 1+1 protection group is provisioned.
- Step 3** 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 4** Click **Apply**.
- Step 5** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.18 AS-CMD

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: AOTS, BPLANE, CLIENT, DS1, DS3, E100T, E1000F, EC1-12, EQPT, FCMR, G1000, ML100T, ML1000, NE, OCH, OCN, OMS, OTS, PWR, TRUNK

The Alarms Suppressed by User Command (AS-CMD) 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; that is, 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:
- Double-click the card to display the card view.
 - 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 AIP that are not in the optical or electrical slots. To clear the alarm:
- In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.
 - In the backplane row, deselect the Suppress Alarms column check box.
 - Click **Apply**.
- Step 8** If the condition is reported for the shelf, cards and other equipment are affected. To clear the alarm:
- In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs if you have not already done so.
 - Click the Suppress Alarms check box located at the bottom of the window to deselect the option.
 - Click **Apply**.
- Step 9** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.19 AS-MT

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: AOTS, CLIENT, DS1, DS3, EC1-12, FCMR, G1000, OCH, OCN, OMS, OTS, TRUNK

The Alarms Suppressed for Maintenance Command (AS-MT) condition applies to OC-N and electrical (traffic) cards and occurs when a port is placed in the out-of-service maintenance (OOS-MT) state for loopback testing operations.

Clear the AS-MT Condition

- Step 1** Complete the [“Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback”](#) procedure on page 2-217.

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

2.7.20 AUD-LOG-LOSS

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

The Audit Trail Log Loss (AUD-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. You will have to off-load (save) the log 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 will be saved in this file. New entries will continue with the next number in the sequence, rather than starting over.
- Step 7** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.21 AUD-LOG-LOW

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: NE

The Audit Trail Log Low (AUD-LOG-LOW) condition occurs when the audit trail log is 80 percent full.



Note

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

2.7.22 AU-LOF

The AU-LOF condition is not used in this platform in this release. It is reserved for future development.

2.7.23 AUTOLSROFF

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

The Auto Laser Shutdown (AUTOLSROFF) 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 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 (IS) for the laser to be on. The laser is off when the safety key is off (labeled 0).



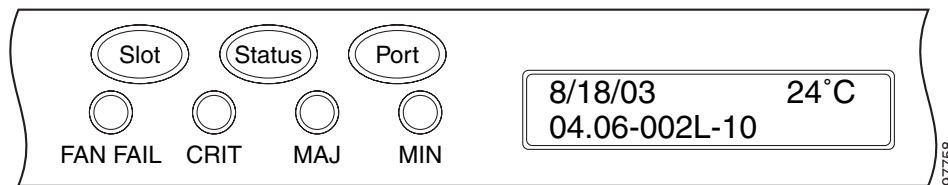
Warning

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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.

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 2-103](#).
- 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 Card” procedure on page 2-219](#) 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.



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.
-

2.7.24 AUTORESET

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

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



Caution

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

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 Card” procedure on page 2-219](#).



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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.



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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.25 AUTOSW-AIS

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

The Automatic path protection Switch Caused by AIS (AUTOSW-AIS) condition indicates that automatic path protection 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 tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The fault condition AIS is raised by the receiving node on each input when it sees the signal 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 2-22.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.26 AUTOSW-LOP (STSMON)

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

The Automatic UPSR Switch Caused by Loss of Pointer (LOP) condition (AUTOSW-LOP) for the STS monitor (STSMON) indicates that automatic path protection protection switching occurred because of the “[LOP-P](#)” alarm on page 2-125. 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 2-125.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.27 AUTOSW-LOP (VT-MON)

- Minor (MN), Service-Affecting (SA)
- Logical Object: VT-MON

The AUTOSW-LOP alarm for the virtual tributary monitor (VT-MON) indicates that automatic path protection protection switching occurred because of the “[LOP-V](#)” alarm on page 2-125. The path protection is configured for revertive switching and reverts to the working path after the fault clears.

Clear the AUTOSW-LOP (VT-MON) Alarm

-
- Step 1** Complete the “[Clear the LOP-V Alarm](#)” procedure on page 2-126.

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

2.7.28 AUTOSW-PDI

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

The Automatic UPSR Switch Caused by Payload Defect Indication (PDI) condition (AUTOSW-PDI) indicates that automatic path protection switching occurred because of a “PDI-P” alarm on page 2-164. 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 2-165.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.29 AUTOSW-SDBER

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

The Automatic UPSR Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition (AUTOSW-SDBER) indicates that a signal degrade [see the “[SD \(CLIENT, TRUNK\)](#)” condition on page 2-178] caused automatic path protection 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-L Condition](#)” procedure on page 2-180.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.30 AUTOSW-SFBER

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

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition (AUTOSW-SFBER) indicates that the “SF (DS1, DS3)” condition on page 2-182 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 2-182.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.31 AUTOSW-UNEQ (STSMON)

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

The Automatic UPSR Switch Caused by Unequipped Path (AUTOSW-UNEQ) 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 2-204.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.32 AUTOSW-UNEQ (VT-MON)

- Minor (MN), Service-Affecting (SA)
- Logical Object: VT-MON

AUTOSW-UNEQ (VT-MON) indicates that the “UNEQ-V” alarm on page 2-206 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) Alarm

- Step 1** Complete the “Clear the UNEQ-V Alarm” procedure on page 2-206.
- Step 2** 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.
-

2.7.33 AWG-DEG

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

The arrayed waveguide gratings (AWG) Temperature Degrade alarm (AWG-DEG) indicates that an internal failure on the multiplexer or demultiplexer heater control circuit causes the AWG temperature to rise above or fall below the degrade threshold.

Clear the AWG-DEG Alarm

- Step 1** This alarm does not immediately affect traffic. But eventually, you will need to complete the “[Physically Replace a Card](#)” procedure on page 2-219 on the reporting card to clear the alarm.



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. Refer to the *Cisco ONS 15454 Procedure Guide* for information.



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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.34 AWG-FAIL

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

The AWG Temperature Fail (AWG-FAIL) alarm indicates that a heater control circuit on the multiplexer or demultiplexer card has failed.

Clear the AWG-FAIL Alarm

- Step 1** Complete the “[Physically Replace a Card](#)” procedure on page 2-219.



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. Refer to the *Cisco ONS 15454 Procedure Guide* for information.



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 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.
-

2.7.35 AWG-OVERTEMP

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

The AWG Over Temperature (AWG-OVERTEMP) alarm occurs in conjunction with the [“AWG-FAIL” alarm on page 2-40](#) when the AWG temperature exceeds 100 degrees C (212 degrees F). The multiplexer or demultiplexer goes into protection mode, disabling the AWG chip heater.

Clear the AWG-OVERTEMP Alarm

- Step 1** Complete the [“Physically Replace a Card” procedure on page 2-219](#).



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. Refer to the *Cisco ONS 15454 Procedure Guide* for information.



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 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.
-

2.7.36 AWG-WARM-UP

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

The AWG Warm-up (AWG-WARM-UP) condition occurs during AWG startup. The length of time needed for the condition to clear varies, depending upon environmental conditions. It can last up to approximately 10 minutes.



Note

AWG-WARM-UP is an informational condition, and does not require troubleshooting unless it does not clear.

2.7.37 BAT-FAIL

- Major (MJ), Service-Affecting (SA)

- Logical Object: PWR

The Battery Fail (BAT-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.
- Step 3** 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.
-

2.7.38 BKUPMEMP

- Critical (CR), Non-Service Affecting (NSA)
- Logical Object: EQPT

The Primary Non-Volatile Backup Memory Failure (BKUPMEMP) alarm refers to a problem with the TCC2 card's flash memory. The alarm occurs when the TCC2 card 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, or the code volume fails cyclic redundancy checking (CRC). CRC is a method to verify for errors in data transmitted to the TCC2.

The BKUPMEMP alarm can also cause the “EQPT” alarm on page 2-69. If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarm.



Caution

It can take up to 30 minutes for software to be updated on a standby TCC2 card.

Clear the BKUPMEMP Alarm

-
- Step 1** Verify that both TCC2 cards are powered and enabled by confirming lighted ACT/SBY LEDs on the TCC2 cards.
- Step 2** If both TCC2 cards are powered and enabled, reset the TCC2 card against which the alarm is raised. If the card is the active TCC2 card, complete the “[Reset Active TCC2 Card and Activate Standby Card](#)” procedure on page 2-217. If the card is the standby TCC2, use the substeps below.
- Right-click the standby TCC2 card in CTC.
 - Choose **Reset Card** from the shortcut menu.
 - Click **Yes** in the Are You Sure dialog box. The card resets, the FAIL LED blinks on the physical card.
 - Wait ten minutes to verify that the card you reset completely reboots.

- Step 3** If the TCC2 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” procedure on page 2-218](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-219](#).
-

2.7.39 BLSROSYNC

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

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

Clear the BLSROSYNC Alarm

- Step 1** Reestablish cabling continuity to the node reporting the alarm. Refer to the *Cisco ONS 15454 Procedure Guide* for cabling information.
- 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 [“EOC” section on page 2-66](#).
- Step 3** 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.
-

2.7.40 CARLOSS (CLIENT)

- Major (MJ), Service-Affecting (SA)
- Logical Object: CLIENT

A Carrier Loss (CARLOSS) alarm on the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card occurs when ITU-T G.709 monitoring is turned off at the client port. It is similar to the [“LOS \(OCN\)” alarm on page 2-132](#).

Clear the CARLOSS (CLIENT) Alarm

- Step 1** From node view, double-click the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card to display card view.
- Step 2** Click the **Provisioning > OTN > OTN Lines** tabs.
- Step 3** Check the check box under the **G.709 OTN** column.
- 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.
-

2.7.41 CARLOSS (EQPT)

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

A CARLOSS on 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 card or the LAN backplane pin connection on the ONS 15454. 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 ONS 15454.

Clear the CARLOSS (EQPT) Alarm

-
- Step 1** If the reporting card is a TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card, verify the type of payload configured:
- Double-click the reporting TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card.
 - Click the **Provisioning > Card** tabs.
 - From the Payload Data Type list, choose the correct payload for the card and click **Apply**.
- 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.
- Step 5** Verify that the optical LAN cable is properly connected and attached to the correct port.
- 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.
- Step 7** If you are unable to establish connectivity, replace the fiber cable with a new known-good 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.

- Step 9** 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.
-

2.7.42 CARLOSS (E100T, E1000F)

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

A CARLOSS on the LAN E100T or E1000F Ethernet (traffic) card is the data equivalent of the “[LOS \(OCN\)](#)” alarm on page 2-132. 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 (traffic) card rather than an Ethernet device, or an improperly installed Ethernet card. Ethernet card ports must be enabled (in service, IS) 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). The database restoration circumstance applies to the E-Series Ethernet cards but not the G1000-4 card, because the G1000-4 card does not use STP and is unaffected by STP reestablishment.



Caution

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

Clear the CARLOSS (E100T, E1000F) Alarm

- Step 1** Verify that the fiber cable is properly connected and attached to the correct port.
- 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.
- 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.
- Step 6** If a valid Ethernet signal is present, complete the “[Remove and Reinsert \(Reseat\) a Card](#)” procedure on page 2-219 for the Ethernet (traffic) card.
- Step 7** If the alarm does not clear, complete the “[Physically Replace a Card](#)” procedure on page 2-219 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 “[Switch Protection Group Traffic with an External Switching Command](#)” procedure on page 2-216 for more information.



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.
- If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, then the reappearing alarm could be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. Perform the following steps unless the Ethernet circuit is part of a manual cross-connect:
- 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.
 - 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 2-217](#) and reconfigure the circuit with the correct circuit size. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.
- Step 9** 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.
-

2.7.43 CARLOSS (G1000)

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

A CARLOSS on the LAN G1000 Ethernet (traffic) card is the data equivalent of the [“LOS \(OCN\)” condition on page 2-132](#). 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 far-end G1000-4 card), it causes the reporting G1000-4 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 far-end 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 2-200 or OC-N alarms or conditions on the end-to-end path normally accompany the CARLOSS (G-Series) alarm.

Refer to the *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 2-201 for more information about alarms that occur when a point-to-point circuit exists between two G1000-4 cards.

Ethernet card ports must be enabled (in service, IS) for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

**Caution**

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

Clear the CARLOSS (G1000) Alarm

- Step 1** Verify that the fiber cable is properly connected and attached to the correct port.
- 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.
- Step 5** If the alarm does not clear, use an Ethernet test set to determine that 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.
- Step 7** If the alarm does not clear and link autonegotiation is enabled on the G1000-4 port, but the autonegotiation process fails, the G1000-4 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:
 - a. Confirm that the attached Ethernet device has autonegotiation enabled and is configured for compatibility with the asymmetric flow control on the G1000-4 card.
 - b. 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 2-200 is also reported, complete the “Clear the TPTFAIL (G1000) Alarm” procedure on page 2-200. 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'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 **Conditions** tab and the **Retrieve Conditions** button.
 - If LPBKTERMINAL is listed for the port, a loopback is provisioned. Go to [Step 11](#). If IS is listed, go to [Step 12](#).

- Step 11** If a loopback was provisioned, complete the “[Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback](#)” procedure on page 2-217.

On the G1000-4 card, 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 LPBKTERMINAL 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 Ethernet manual cross-connect is used when another vendors’ equipment sits between ONS 15454s, 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.

- Right-click anywhere in the row of the CARLOSS alarm.
 - Right-click or left-click **Select Affected Circuits** in the shortcut menu that appears.
 - Record the information in the type and size columns of the highlighted circuit.
 - 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.
 - Log into the ONS 15454 at the other end of the Ethernet manual cross-connect.
 - Double-click the Ethernet (traffic) 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.
 - 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.
 - If one of the circuit sizes is incorrect, complete the “[Delete a Circuit](#)” procedure on page 2-217 and reconfigure the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed procedures to create circuits.
- Step 13** If a valid Ethernet signal is present, complete the “[Remove and Reinsert \(Reseat\) a Card](#)” procedure on page 2-219.
- Step 14** If the alarm does not clear, complete the “[Physically Replace a Card](#)” procedure on page 2-219 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.

**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 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.

2.7.44 CARLOSS (ML100T, ML1000)

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

A CARLOSS on the ML100T or ML1000 Ethernet (traffic) card is the data equivalent of the [“LOS \(OCN\)” alarm on page 2-132](#). 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 IOS command line interface (CLI) as a no-shutdown port and one of the following items 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 IOS interface, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide, Release 4.6*.

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.
- 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 reenable the Ethernet port by performing a “shutdown” and then a “no shutdown” on the IOS CLI. Autonegotiation will restart.
- Step 6** If the alarm does not clear, complete the [“Perform a Facility \(Line\) Loopback on a Source DS-N Port \(West to East\)” procedure on page 1-8](#).

Step 7 If the problem persists with the loopback installed, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-219](#).

Step 8 If the alarm does not clear, complete the [“Physically Replace a Card” procedure on page 2-219](#).

**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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.

**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 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.

2.7.45 CARLOSS (TRUNK)

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

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

Clear the CARLOSS (TRUNK) Alarm

Step 1 Complete the [“Clear the CARLOSS \(CLIENT\) Alarm” procedure on page 2-43](#).

Step 2 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.

2.7.46 CASETEMP-DEG

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

The Case Temperature Degrade (CASETEMP-DEG) alarm occurs when a card detects a case temperature value outside the desired range (–5 to 65 degrees C or 23 to 149 degrees F).

Clear the CASETEMP-DEG Alarm

Step 1 If a FAN alarm is also reported, complete the [“Clear the FAN Alarm” procedure on page 2-83](#).

Step 2 If no FAN alarm is reported, complete the [“Replace the Air Filter” procedure on page 3-5](#).

- Step 3** 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.

2.7.47 CKTDOWN

- Critical (CR), Service-Affecting (SA)
- Logical Object: UCP-CKT

The unified control plane (UCP) Circuit Down (CKTDOWN) alarm applies to logical circuits created within the UCP between devices. It occurs when there is signaling failure across a UCP interface. The failure can be caused by a number of things, such as failure to route the call within the core network. In that case, the alarm cannot be resolved from the ONS 15454 because it is an edge device.

Clear the CKTDOWN Alarm

- Step 1** Ensure that the channel to neighbor has been provisioned with the correct IP address:

- In node view, click the **Provisioning > UCP > Neighbor** tabs.
- View the entries to find out whether the node you are trying to contact is listed.
The node name is listed under the Name column and the IP address is listed under the Node ID column. If the Node ID says 0.0.0.0 and the Enable Discovery check box is selected, the node could not automatically identify the IP address. Ping the node to ensure that it is physically and logically accessible.
- Click **Start > Programs > Accessories > Command Prompt** to open an MS-DOS command window for pinging the neighbor.
- At the command prompt (C:\>), type:

```
ping {node-DNS-name | node-IP-address}
```

If you typed the domain name services (DNS) name and the ping was successful, you will see:

```
pinging node-dns-name.domain-name.com. node-IP-address with 32 bytes of data:
Reply from IP-address: bytes=32 time=10ms TTL=60
Reply from IP-address: bytes=32 time=10ms TTL=60
Reply from IP-address: bytes=32 time=10ms TTL=60
Reply from IP-address: bytes=32 time=10ms TTL=60
```

```
Ping statistics for IP-address:
Packets sent = 4 Received = 4 Lost = 0 (0% lost),
Approximate round trip time in milli-seconds:
Minimum = minimum-ms, Maximum = maximum-ms, Average = average-ms
```

If you typed the IP address and the ping command is successful, the result will look similar but will not include the DNS name in the first line.

- If your DNS name or IP address ping was successful, IP access to the node is confirmed, but your neighbor configuration is wrong. Delete the neighbor by selecting it in the window and clicking **Delete**.
- If the ping was unsuccessful, you will receive the following reply for each try:

Request timed out.

A negative reply indicates that the neighbor node is not physically or logically accessible. Resolve the access problem, which is probably a cabling issue.

- Step 2** If the neighbor has not been provisioned, or if you had to delete the neighbor, create one:
- In the Provisioning > UCP > Neighbor tabs, click the **Create** button.
 - In the Neighbor Discovery window, enter the node's DNS node name in the Neighbor Name field. Leave the Enable Discovery check box checked (default setting) if you want the neighbor to be discovered through the network.
 - Click **OK**.
The node is listed in the Neighbor column list. If the neighbor discovery worked, the neighbor IP address is listed in the Node ID column. If it is not successful, the column lists 0.0.0.0.
- Step 3** If neighbor discovery is enabled, ensure that the neighbor node ID and remote Internet protocol (IP) control channel (IPCC) have been discovered correctly.
- Step 4** Click the **Provisioning > UCP > IPCC** tabs and view the IPCC listing. If the IPCC has been created correctly, the Remote IP column contains the neighbor's IP address.
- Step 5** If the neighbor IP address is not correctly discovered, the field contains 0.0.0.0.
- Click the entry to select the neighbor IP address and click **Delete**.
 - If you get an error that will not allow you to delete the IPCC, you must delete the neighbor and recreate it. Click the **Neighbor** tab.
 - Click to select the neighbor and click **Delete**.
 - Go back to [Step 2](#) to recreate the neighbor.
- Step 6** If remote IPCC has not been discovered, or if it had to be deleted, create the connection:
- In the Provisioning > UCP > IPCC tabs, click **Create**.
 - In the Unified Control Plane Provisioning window, click **Next**.
 - If no IPCCs are listed, click **Create**.
 - In the Create New IPCC window, click the DCC termination corresponding to the core network interface.
Leave the SDCC radio button selected (as long as DCCs have been created on the node) and leave the Leave Unchanged radio button selected.
 - Click **OK**. The IPCC is listed in the Unified Control Plane Provisioning window.
 - Click the neighbor to select it, and click **Next**.
 - Choose the UCP interface [for example, Slot 5 (OC-48), port 1] where the core network is connected from the pull-down menu. The field default is the node where you are logged in.
 - Choose the UCP interface TNA address type. The default is IPv4. The address field lists the login node IP address by default.
 - Click **Finish**. If creation is successful, the Remote ID column in the IPCC tab will contain the neighbor's IP address.
- Step 7** Ensure that the local and remote interface IDs have been provisioned correctly:
- Click the **Interface** tab. View the slot and port listed in the Interface column [for example, Slot 5 (OC48), port 1].
 - Compare the listed interface listed with the IPCC tab SDCC column entry.

- Step 8** If the Interface column is not the same as the SDCC column entry, click the entry in the Interface window to select it and click **Delete**.
- Step 9** Click **Next**.
- Step 10** In the Existing CCIDs list, click the IPCC containing the DCC connection. Click **Next**.
The correct interface for the selected CCID is shown in the UPC Interface field, and the correct IP address information for the login node is shown by default in the other fields. Click **Finish**.
- Step 11** If you completed all of these steps and verified the information, the alarm could be the result of a misconfiguration in the core network. Contact the core site administrators.
- Step 12** 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.
-

2.7.48 CLDRESTART

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

The Cold Restart (CLDRESTART) condition occurs when a card is physically removed and inserted, replaced, or when the ONS 15454 is first powered up.



Caution

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

Clear the CLDRESTART Condition

- Step 1** If the condition fails to clear after the card reboots, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-219](#).
- Step 2** If the condition does not clear, complete the [“Physically Replace a Card” procedure on page 2-219](#) 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.



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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.49 COMIOXC

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

The Input/Output Slot To Cross-Connect Communication Failure (COMIOXC) 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 2-218 on the reporting XC10G cross-connect card. For the LED behavior, see the “[Non-DWDM Card LED Activity During Reset](#)” section on page 2-212.
- Step 2** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the “[Non-DWDM Card LED State After Successful Reset](#)” section on page 2-213.
- 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 2-216.
- Step 4** Complete the “[Remove and Reinsert \(Reseat\) a Card](#)” procedure on page 2-219 for the reporting cross-connect card.
- Step 5** If the alarm does not clear, complete the “[Physically Replace a Card](#)” procedure on page 2-219 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 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.
-

2.7.50 COMM-FAIL

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

The Plug-In Module (card) Communication Failure (COMM-FAIL) alarm indicates that there is a communication failure between the TCC2 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 2-218 for the reporting card.
- Step 2** If the alarm does not clear, complete the “[Physically Replace a Card](#)” procedure on page 2-219 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.

**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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.51 CONTBUS-A-18

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

A Communication Failure from TCC2 A Slot to TCC2 Slot A (CONTBUS-A-18) alarm occurs when the main processor on the TCC2 card in Slot 7 (termed TCC A) loses communication with the coprocessor on the same 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 at the lower-right outside edge of the shelf assembly.

Clear the CONTBUS-A-18 Alarm

- Step 1** Complete the [“Reset Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#) to make the TCC2 in Slot 11 active.
- Step 2** Wait approximately 10 minutes for the TCC2 in Slot 7 to reset as the standby TCC2. Verify that the standby LED is illuminated before proceeding to the next step.
- Step 3** Position the cursor over the TCC2 card in Slot 11 and complete the [“Reset Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#) to make the standby TCC2 in Slot 7 active.
- Step 4** If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2” procedure on page 2-218](#). If the TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-219](#).

2.7.52 CONTBUS-B-18

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

A Communication Failure from TCC2 B Slot to TCC2 B Slot (CONTBUS-B-18) alarm occurs when the main processor on the TCC2 card in Slot 11 (termed TCC B) loses communication with the coprocessor on the same 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 at the lower-right outside edge of the shelf assembly.

Clear the CONTBUS-B-18 Alarm

-
- Step 1** Position the cursor over the TCC2 card in Slot 11 and complete the [“Reset Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#) to make the TCC2 in Slot 7 active.
- Step 2** Wait approximately 10 minutes for the TCC2 in Slot 11 to reset as the standby TCC2. Verify that the standby LED is illuminated before proceeding to the next step.
- Step 3** Position the cursor over the TCC2 card in Slot 7 and complete the [“Reset Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#) to make the standby TCC2 in Slot 11 active.
- Step 4** If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1 800 553-2447). If the TAC technician tells you to reseat the card, complete the [“Reset Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#). If the TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-219](#).
-

2.7.53 CONTBUS-IO-A

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

A TCC A to Shelf Slot Communication Failure (CONTBUS-IO-A) alarm occurs when the active TCC2 card in Slot 7 (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 might appear briefly when the ONS 15454 switches to the protect TCC2 card. In the case of a TCC2 protection switch, the alarm clears after the other cards establish communication with the new active TCC2 card. If the alarm persists, the problem is with the physical path of communication from the TCC2 card to the reporting card. The physical path of communication includes the TCC2 card, the other card, and the backplane.

**Caution**

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

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 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 2-148](#) for the reporting card.

- Step 2** If the alarm object is any single card slot other than the standby TCC2 in Slot 11, perform a CTC reset of the object card. Complete the [“Reset a Traffic Card in CTC” procedure on page 2-218](#). For the LED behavior, see the [“Non-DWDM Card LED Activity During Reset” section on page 2-212](#).
- Step 3** If the alarm object is the standby TCC2 in Slot 11, perform a soft reset of this card:
- Right-click the Slot 11 TCC2 card.
 - Choose **Reset Card** from the shortcut menu.
 - Click **Yes** in the confirmation dialog box. Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
- Step 4** If CONTBUS-IO-A is raised on several cards at once, complete the [“Reset Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#).
- 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. For LED appearance, see the [“Non-DWDM Card LED State After Successful Reset” section on page 2-213](#).
- Step 6** If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-219](#) for the reporting card.
- Step 7** If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1 800 553-2447). If the TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2” procedure on page 2-218](#). If the TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-219](#).
-

2.7.54 CONTBUS-IO-B

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

A TCC B to Shelf Slot Communication Failure (CONTBUS-IO-B) alarm occurs when the active TCC2 card in Slot 11 (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 card. In the case of a TCC2 protection switch, the alarm clears after the other cards establish communication with the new active TCC2 card. If the alarm persists, the problem is with the physical path of communication from the TCC2 card to the reporting card. The physical path of communication includes the TCC2 card, the other card, and the backplane.



Caution

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

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 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 2-148](#) for the reporting card.

- Step 2** If the alarm object is any single card slot other than the standby TCC2 in Slot 7, perform a CTC reset of the object card. Complete the [“Reset a Traffic Card in CTC” procedure on page 2-218](#). For the LED behavior, see the [“Non-DWDM Card LED Activity During Reset” section on page 2-212](#).
- Step 3** If the alarm object is the standby TCC2 in Slot 7, perform a soft reset of this card:
- Right-click the Slot 7 TCC2 card.
 - Choose **Reset Card** from the shortcut menu.
 - Click **Yes** in the confirmation dialog box. Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.
- Step 4** If CONTBUS-IO-B is raised on several cards at once, complete the [“Reset Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#).
- 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. For LED appearance, see the [“Non-DWDM Card LED State After Successful Reset” section on page 2-213](#).
- Step 6** If the CTC reset does not clear the alarm, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-219](#) for the reporting card.
- Step 7** If the reset card has not rebooted successfully, or the alarm has not cleared, call TAC (1 800 553-2447). If the TAC technician tells you to reseat the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2” procedure on page 2-218](#). If the TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-219](#).

2.7.55 CTNEQPT-MISMATCH

- 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, an XC card may be preprovisioned in Slot 10, but an XCVT may be physically installed.

The alarm is raised against a card that is mismatched with the card. For example, CTNEQPT-MISMATCH is raised in the following situations:

- An XC card is replaced with an XCVT or XC10G card.
- 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. (For example, you might have an XC in Slot 8 and an XC10G in Slot 10 while you are upgrading Slot 10.)



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 R4.6 and replace an XC with XCVT or XC10G, or an XCVT with an XC10G, the CTNEQPT-MISMATCH condition is raised but it will be 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 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 Card” procedure on page 2-219](#) 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).
-

2.7.56 CTNEQPT-PBPROT

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

The Interconnection Equipment Failure Protect Cross-Connect Card Payload Bus (CTNEQPT-PBPROT) alarm indicates a failure of the main payload between the 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, the reporting traffic card, the TCC2 card, or the backplane.

**Note**

If all traffic cards show CTNEQPT-PBPROT alarm, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2” procedure on page 2-218](#) for the standby TCC2 card. If the reseat fails to clear the alarm, complete the [“Physically Replace a Card” procedure on page 2-219](#) for the standby TCC2 card. Do not physically reseat an active TCC2 card. Reseating the TCC2 disrupts traffic.

**Note**

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

**Caution**

It can take up to 30 minutes for software to be updated on a standby TCC2 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 at the lower-right outside edge of the shelf assembly.

Clear the CTNEQPT-PBPROT Alarm

-
- Step 1** Perform a CTC reset on the standby XC10G cross-connect card. Complete the [“Reset a Traffic Card in CTC” procedure on page 2-218](#). For the LED behavior, see the [“Non-DWDM Card LED Activity During Reset” section on page 2-212](#).
- Step 2** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the [“Non-DWDM Card LED State After Successful Reset” section on page 2-213](#).
If the cross-connect reset is not complete and error-free or if the TCC2 reboots automatically, call Cisco TAC (1 800 553-2447).
- Step 3** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-219](#) for the standby cross-connect card.
- Step 4** 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 status are displayed in the list.
- Step 5** If the reporting traffic card is the active card in the protection group, complete the [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#). After you move traffic off the active card, or if the reporting card is standby, continue with the following steps.
- Step 6** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-218](#) on the reporting card. For the LED behavior, see the [“Non-DWDM Card LED Activity During Reset” section on page 2-212](#).
- Step 7** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the [“Non-DWDM Card LED State After Successful Reset” section on page 2-213](#).
- Step 8** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-219](#) for the reporting card.
- Step 9** Complete the [“Clear a Protection Group External Switching Command” procedure on page 2-216](#).
- Step 10** If the alarm does not clear, complete the [“Physically Replace a Card” procedure on page 2-219](#) 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.

**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 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.
-

2.7.57 CTNEQPT-PBWORK

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

The Interconnection Equipment Failure Working Cross-Connect Card Payload Bus (CTNEQPT-PBWORK) alarm indicates a failure in the main payload bus between the 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, the reporting traffic card, or the backplane.


Note

If all traffic cards show CTNEEQPT-PBWORK alarm, complete the [“Reset Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#) for the active TCC2 card and then complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2” procedure on page 2-218](#). If the reseat fails to clear the alarm, complete the [“Physically Replace a Card” procedure on page 2-219](#) for the TCC2 card. Do not physically reseat an active TCC2 card; it disrupts traffic.


Note

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


Caution

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

Clear the CTNEQPT-PBWORK Alarm

- Step 1** Complete the [“Side Switch the Active and Standby XC10G Cross-Connect cards” procedure on page 2-216](#) for the active XC10G cross-connect card.


Note

After the active cross-connect goes into standby, the original standby slot becomes active. The active card ACT/SBY LED becomes green.

- Step 2** Complete the [“Reset a Traffic Card in CTC” procedure on page 2-218](#) for the reporting card. For the LED behavior, see the [“Non-DWDM Card LED Activity During Reset” section on page 2-212](#).
- Step 3** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the [“Non-DWDM Card LED State After Successful Reset” section on page 2-213](#).
- Step 4** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-219](#) for the standby cross-connect card.


Note

The ACT/SBY LED of the active card is green. The ACT/SBY LED of the standby card is amber.

- Step 5** If the alarm does not clear and the reporting traffic card is the active card in the protection group, complete the [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#). If the card is standby, or if you have moved traffic off the active card, proceed with the following steps.

- Step 6** Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-218 for the reporting card. For the LED behavior, see the “[Non-DWDM Card LED Activity During Reset](#)” section on page 2-212.
- Step 7** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the “[Non-DWDM Card LED State After Successful Reset](#)” section on page 2-213.
- Step 8** If the CTC reset does not clear the alarm, complete the “[Remove and Reinsert \(Reseat\) a Card](#)” procedure on page 2-219 for the reporting card.
- Step 9** If you switched traffic, complete the “[Clear a Protection Group External Switching Command](#)” procedure on page 2-216.
- Step 10** If the alarm does not clear, complete the “[Physically Replace a Card](#)” procedure on page 2-219 for the 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 11** If the alarm does not clear, complete the “[Physically Replace a Card](#)” procedure on page 2-219 for the reporting traffic card.
- Step 12** 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.
-

2.7.58 DATAFLT

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

The Software Data Integrity Fault (DATAFLT) alarm occurs when the TCC2 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 Active TCC2 Card and Activate Standby Card](#)” procedure on page 2-217.
- Step 2** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.59 DBOSYNC

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

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

**Caution**

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

Clear the DBOSYNC Alarm

-
- Step 1** Save a backup copy of the active TCC2 database. Complete the “Back Up the Database” procedure in the *Cisco ONS 15454 Procedure Guide*.
- Step 2** Make a minor provisioning change to the active database to see if applying a provisioning change clears the alarm:
- In node view, click the **Provisioning > General > General** tabs.
 - 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.60 DSP-COMM-FAIL

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

The digital signal processor (DSP) Communication Failure alarm (DSP-COMM-FAIL) indicates that there is a communications failure between an MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card microprocessor and the on-board DSP chip that controls the trunk (DWDM) port. This alarm typically occurs after a DSP code upgrade.

The alarm is temporary and does not require user action. The MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G 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_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card raises the “[DSP-FAIL](#)” alarm on page 2-63, and could affect traffic.

**Note**

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

2.7.61 DSP-FAIL

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

The DSP Failure (DSP-FAIL) alarm indicates that a “[DSP-COMM-FAIL](#)” alarm on page 2-63 has persisted for an extended period on an MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card. It indicates that the card is faulty.

Clear the DSP-FAIL Alarm

Step 1 Complete the “[Physically Replace a Card](#)” procedure on page 2-219 for the reporting MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G 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 “[Switch Protection Group Traffic with an External Switching Command](#)” procedure on page 2-216 for more information.



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 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.

2.7.62 DS3-MISM

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

The DS-3 Frame Format Mismatch (DS3-MISM) condition indicates a frame format mismatch on a signal transiting the DS3XM-6 card. The condition occurs when the provisioned line type and incoming signal frame format type do not match. For example, if the line type is set to C Bit for a DS3XM-6 card, and the incoming signal’s 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 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.

Step 4 If the Line Type pull-down menu does not match the expected incoming signal, select the correct Line Type in the pull-down menu.

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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.63 DUP-IPADDR

- Major (MJ), 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** In node view, click the **Provisioning > Network > General** tabs.
- Step 2** In the IP Address field, change the IP address to a unique number.
- Step 3** Click **Apply**.
- 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).
-

2.7.64 DUP-NODENAME

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The Duplicate Node Name (DUP-NODENAME) alarm indicates that the alarmed node's 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.65 EHIBATVG

- Major (MJ), Service-Affecting (NSA)
- Logical Object: PWR

The Extreme High Voltage Battery (EHIBATVG) alarm occurs in a –48 VDC environment when a battery lead's 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*.)

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 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.
-

2.7.66 ELWBATVG

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

The Extreme Low Voltage Battery (ELWBATVG) alarm occurs in a –48 VDC environment when a battery lead's 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*.)

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 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.
-

2.7.67 EOC

- Major (MJ), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The SONET Data Communications Channel (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 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 (IS) for the laser to be on. The laser is off when the safety key is off (labeled 0).



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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.



Caution

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



Note

If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place. The circuit will be 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 2-128 is also reported, complete the “Clear the LOS (DS1) Alarm” procedure on page 2-128.
- Step 2** If the alarm does not clear on the reporting node, verify the physical connections between the cards and the fiber-optic cables that are configured to carry DCC traffic.
- Step 3** If the physical connections are correct and configured to carry DCC traffic, verify that both ends of the fiber span have in-service (IS) ports by checking that the ACT LED on each OC-N card is illuminated.
- Step 4** If the ACT LEDs on OC-N cards are illuminated, complete the “Verify or Create Node DCC Terminations” procedure on page 2-214 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:
 - a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.
A green LED indicates an active card. An amber LED indicates a standby card.
 - b. To determine whether the 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 State column lists the port as IS.

- e. If the State column lists the port as OOS, click the column and click **IS** from the pull-down menu. 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.

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 [“OC-N Card Transmit and Receive Levels”](#) section on page 1-102 non-DWDM card levels and see the *Cisco ONS 15454 Reference Manual* 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 “Install the Fiber-Optic Cables” procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 10 If fiber connectors are properly fastened and terminated, complete the [“Reset Active TCC2 Card and Activate Standby Card”](#) procedure on page 2-217.

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

Resetting the active TCC2 switches control to the standby TCC2. If the alarm clears when the ONS 15454 switches to the standby TCC2, the user can assume that the original active TCC2 is the cause of the alarm.

Step 11 If the TCC2 reset does not clear the alarm, delete the problematic DCC termination:

- a. From card view, click **View > Go to Previous View** if you have not already done so.
- a. Click the **Provisioning > DCC/GCC/OSC** tabs.
- b. Highlight the problematic DCC termination.
- c. Click **Delete**.
- d. Click **Yes** in the confirmation dialog box.

Step 12 Recreate the DCC termination. Refer to the *Cisco ONS 15454 Procedure Guide* 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”](#) procedure on page 2-218. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card”](#) procedure on page 2-219.

2.7.68 EOC-L

- Major (MJ), 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 (IS) for the laser to be on. The laser is off when the safety key is off (labeled 0).

**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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.

**Caution**

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

**Note**

If a circuit shows an incomplete state when the EOC alarm is raised, it occurs when the logical circuit is in place. The circuit will be 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 2-67](#).
- Step 2** 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” procedure on page 2-218](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-219](#).

2.7.69 EQPT

- Critical (CR), Service-Affecting (SA)
- Logical Objects: AICI-AIE, EQPT

An Equipment Failure (EQPT) alarm indicates that a hardware failure has occurred on the reporting card. If the EQPT alarm occurs with a BKUPMEMP alarm, refer to the [“BKUPMEMP” section on page 2-42](#). The BKUPMEMP procedure also clears the EQPT 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 at the lower-right outside edge of the shelf assembly.

Clear the EQPT Alarm

-
- Step 1** Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-218 for the reporting card. For the LED behavior, see the “[Non-DWDM Card LED Activity During Reset](#)” section on page 2-212.
- Step 2** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the “[Non-DWDM Card LED State After Successful Reset](#)” section on page 2-213.
- Step 3** If the CTC reset does not clear the alarm, complete the “[Remove and Reinsert \(Reseat\) a Card](#)” procedure on page 2-219 for the reporting card.
- Step 4** If the physical reseat of the card fails to clear the alarm, complete the “[Physically Replace a Card](#)” procedure on page 2-219 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 “[Switch Protection Group Traffic with an External Switching Command](#)” procedure on page 2-216 for more information.



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 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.
-

2.7.70 EQPT-MISS

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

The Replaceable Equipment or Unit Missing (EQPT-MISS) alarm is reported against the fan-tray assembly unit. It indicates that the replaceable fan-tray assembly is missing or not fully inserted or that the ribbon cable connecting the AIP to the system board may be 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 at the lower-right outside 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 “[Remove and Reinsert Fan-Tray Assembly](#)” procedure on page 2-220.
- 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*.
- 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 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.
-

2.7.71 ERFI-P-CONN

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

The three-bit enhanced remote failure indication (ERFI) Path Connectivity condition (ERFI-P-CONN) is triggered on DS-1, DS-3, and VT circuits when the “UNEQ-P” alarm on page 2-204 and the “TIM-P” alarm on page 2-199 are raised on the transmission signal.

Clear the ERFI-P-CONN Condition

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

2.7.72 ERFI-P-PAYLD

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

The ERFI Path Payload (ERFI-P-PAYLD) condition is triggered on DS-1, DS-3, and VT circuits when the “PLM-P” alarm on page 2-167 alarm is raised on the transmission signal.

Clear the ERFI-P-PAYLD Condition

- Step 1** Complete the “Clear the PLM-P Alarm” procedure on page 2-167. This should clear the ERFI condition.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.73 ERFI-P-SRVR

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

The ERFI Path Server (ERFI-P-SRVR) condition is triggered on DS-1, DS-3, and VT circuits when the “AIS-P” alarm on page 2-22 or the “LOP-P” alarm on page 2-125 is raised on the transmission signal.

Clear the ERFI-P-SRVR Condition

-
- Step 1** Complete the [“Clear the LOP-P Alarm” procedure on page 2-125](#). This should clear the ERFI condition.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.74 ERROR-CONFIG

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

The Error in Startup Configuration (ERROR-CONFIG) alarm applies to the ML-Series Ethernet (traffic) 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.

For information about provisioning the ML-Series Ethernet cards from the IOS interface, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide, Release 4.6*.

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 *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide, Release 4.6*.
- Step 2** Upload the configuration file to the TCC2:
- 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 2-218](#).
- Step 4** If the alarm does not clear or if your configuration file was correct according to the installed card, start an 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 *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide* 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.75 ETH-LINKLOSS

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

The Rear Panel Ethernet Link Removed (ETH-LINKLOSS) 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* for instructions to install this cable.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.76 E-W-MISMATCH

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

A Procedural Error Mismatch East/West Direction (E-W-MISMATCH) alarm occurs when nodes in a ring have an east slot misconnected to another east slot or a west slot 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* for more information about configuring 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).

**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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.

- Step 10** 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.

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 2-213 to identify the node ID, ring name, and the slot and port in the East Line list and West Line columns. Record the above information.
- Step 4** Click **View > Go to Network View**.
- Step 5** Delete and recreate the BLSR:
- Click the **Provisioning > BLSR** tabs.
 - Click the row from [Step 3](#) to select it and click **Delete**.
 - Click **Create BLSR**.
 - Fill in the ring name and node ID from the information collected in [Step 3](#).
 - Click **Finish** in the BLSR Creation window.
- Step 6** Display node view and click the **Maintenance > BLSR** tabs.
- Step 7** Change the West Line pull-down menu to the slot you recorded for the East Line in [Step 3](#).
- Step 8** Change the East Line pull-down menu 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 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.
-

2.7.77 EXCCOL

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

The Excess Collisions on the LAN (EXCCOL) 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 card. The problem causing the alarm is external to the ONS 15454.

Troubleshoot the network management LAN connected to the TCC2 card for excess collisions. You may 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 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 card and the network management LAN.

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

2.7.78 EXERCISE-RING-FAIL

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

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



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 2-123, the “LOS (OCN)” alarm on page 2-132, or BLSR alarms.
- Step 2** Reissue the Exercise Ring command:
- Click the **Maintenance > BLSR** tabs.
 - Click the row of the affected ring under the West Switch column.
 - Select **Exercise Ring** in the pull-down menu.
- 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).
-

2.7.79 EXERCISE-SPAN-FAIL

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

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



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 2-123, the “LOS (OCN)” alarm on page 2-132, or a BLSR alarm.
- Step 2** Reissue the Exercise Span command:
- 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 pull-down menu.
- 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).
-

2.7.80 EXT

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

A Failure Detected External to the NE (EXT) alarm occurs because an environmental alarm is present. For example, a door could be open or flooding may 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** Click the **Maintenance** tab to gather further information about the EXT alarm.
- Step 3** Perform your standard operating procedure for the environmental condition.
- 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).
-

2.7.81 EXTRA-TRAF-PREEMPT

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

An Extra Traffic Preempted (EXT-TRAF-PREEMPT) alarm occurs on OC-N cards in two-fiber and four-fiber BLSRs because 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 *Cisco ONS 15454 Procedure Guide*.
- 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 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.
-

2.7.82 FAILTOSW

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, EQPT, OCN, TRUNK

The Failure to Switch to Protection (FAILTOSW) condition occurs when a working electrical or optical (traffic) card cannot switch to the protect card in a 1:N, Y-cable, or splitter protection group because another working electrical or optical 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 1:N 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 or optical (traffic) card that is reporting the higher priority alarm by following the [“Physically Replace a Card” procedure on page 2-219](#). This card is the working electrical or optical card using the 1:N card protection and not reporting FAILTOSW.

Replacing the working electrical or optical 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.



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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.



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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.83 FAILTOSW-PATH

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

The FAILTOSW Path (FAILTOSW-PATH) condition occurs when the working path does not switch to the protection path on a path protection. Common causes of the FAILTOSW-PATH alarm include a missing or defective protection card or a lockout set on one of the path protection nodes.



Caution

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

Clear the FAILTOSW-PATH Condition in a Path Protection Configuration

- Step 1** Look up and clear the higher priority alarm. Clearing this condition frees the standby card and clears the FAILTOSW-PATH 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 Card” procedure on page 2-219](#). 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.



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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.84 FAILTOSWR

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

The FAILTOSW Ring (FAILTOSW-RING) condition occurs when a ring switch did not complete because of internal APS problems.

FAILTOSWR clears when one of the following situations occurs:

- a physical card pull of the active TCC card (done under TAC supervision);
- a node power cycle;
- a higher priority event such as an external switch command;

- the next ring switch succeeds;
- or, the cause of the APS switch (such as the “SD (DS1, DS3)” condition on page 2-178 or the “SF (DS1, DS3)” condition on page 2-182) 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).

**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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.

Clear the FAILTOSWR Condition in a Four-Fiber 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 pull-down menu.
- 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 near-end 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:
- Confirm that the OC-N card shows a green LED in CTC or on the physical card.
A green LED indicates an active card. An amber LED indicates a standby card.
 - Double-click the card in CTC to display the card view.
 - Click the **Provisioning > Line** tabs.
 - Verify that the State column lists the port as IS.
 - If the State column lists the port as OOS, 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.
- 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 optical (traffic) card. It could be necessary to manually switch traffic carrying circuits over to a protection path.

- 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*.
- 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's receiver specifications. The “[OC-N Card Transmit and Receive Levels](#)” section on [page 1-102](#) 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 Card](#)” procedure on [page 2-219](#) 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 “[Switch Protection Group Traffic with an External Switching Command](#)” procedure on [page 2-216](#) for more information.

**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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.85 FAILTOSWS

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

The FAILTOSW Span (FAILTOSWS) 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 TCC card (done under TAC supervision);
- a node power cycle;
- a higher priority event such as an external switch command occurs;
- the next span switch succeeds;
- or, the cause of the APS switch (such as the “[SD \(DS1, DS3\)](#)” condition on [page 2-178](#) or the “[SF \(DS1, DS3\)](#)” condition on [page 2-182](#)) 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.

- c. Click the row of the affected span under the East Switch or West Switch column.
 - d. Select **Exercise Span** in the pull-down menu.
- 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 near-end node and click the **Maintenance > BLSR** tabs.
- Step 5** Record the OC-N cards listed under West Line and East Line. Ensure that these OC-N cards are active and in service:
- a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.
A green LED indicates an active card. An amber 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 State column lists the port as IS.
 - e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.
- Step 6** If the OC-N cards are active and in service, verify fiber continuity to the ports on the recorded cards.
- Step 7** If fiber continuity to the ports is okay, verify that the correct port is in service:
- a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.
A green LED indicates an active card. An amber 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 State column lists the port as IS.
 - e. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.
- Step 8** If the correct port is 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.

**Caution**

Using an optical test set disrupts service on the optical (traffic) card. It could be necessary to manually switch traffic carrying circuits over to a protection path.

- 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*.
- 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's receiver specifications. The "[OC-N Card Transmit and Receive Levels](#)" section on [page 1-102](#) 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 Card](#)" procedure on [page 2-219](#) 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 “[Switch Protection Group Traffic with an External Switching Command](#)” procedure on page 2-216 for more information.

**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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.86 FAN


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

The Fan Failure (FAN) 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 ONS 15454. 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 at the lower-right outside edge of the shelf assembly.

Clear the FAN Alarm

- Step 1** Determine whether the air filter to see whether it needs replacement. Complete the “[Inspect, Clean, and Replace the Reusable Air Filter](#)” procedure on page 3-5.
- Step 2** If the filter is clean, complete the “[Remove and Reinsert Fan-Tray Assembly](#)” procedure on page 2-220.
-  **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 3-10.
- Step 4** If the replacement fan-tray assembly does not operate correctly, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.7.87 FANDEGRADE

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: FAN

The Partial Fan Failure Speed Control Degradation (FANDEGRADE) alarm occurs if fan speed for one of the fans in the fan-tray assembly falls under 500 RPM when read by a tachometry counter.

Clear the FANDEGRADE Alarm

-
- Step 1** Complete the “[Clear the FAN Alarm](#)” procedure on page 2-83.
- Step 2** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.88 FE-AIS

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

The Far-End AIS (FE-AIS) condition occurs when an AIS has occurred at the far-end node. FE-AIS usually occurs in conjunction with a downstream LOS alarm (see the “[LOS \(OCN\)](#)” alarm on page 2-132).

Generally, any AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The fault condition AIS is raised by the receiving node on each input when it sees the signal 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 2-22.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.89 FEC-MISM

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

The forward error correction (FEC) Mismatch alarm (FEC-MISM) occurs if one end of a span using MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, 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, or TXPP_MR_2.5G card.
 - Step 2** Click the **Provisioning > OTN > OTN Lines** tab.
 - Step 3** Check the FEC column check box.
 - Step 4** Verify that the far-end card is configured the same way by repeating [Step 1](#) through [Step 3](#).
 - Step 5** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.90 FE-DS1-MULTLOS

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

The Far-End Multiple DS-1 LOS Detected (FE-DS1-MULTLOS) condition occurs when multiple DS-1 signals are lost on a far-end DS-1 card. The prefix FE means the main alarm is occurring at the far-end 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 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.91 FE-DS1-NSA

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

The Far End DS-1 Equipment Failure Non-Service Affecting (FE-DS1-NSA) condition occurs when a far-end 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 far-end 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 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.92 FE-DS1-SA

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

The Far End DS-1 Equipment Failure Service Affecting (FE-DS1-SA) condition occurs when there is a far-end 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 far-end 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.93 FE-DS1-SNGLLOS

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

The Far-End Single DS-1 LOS (FE-DS1-SNGLLOS) condition occurs when a single DS-1 signal is lost on far-end DS-1 equipment. Signal loss also causes the “LOS (OCN)” alarm on page 2-132. The prefix FE in an alarm or condition means the main alarm is occurring at the far-end 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.94 FE-DS3-NSA

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

The Far End DS-3 Equipment Failure Non-Service Affecting (FE-DS3-NSA) condition occurs when a far-end DS-3 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 far-end 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.95 FE-DS3-SA

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

The Far End DS-3 Equipment Failure Service Affecting (FE-DS3-SA) condition occurs when there is a far-end equipment failure on a DS-3 card 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 far-end 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.96 FE-EQPT-NSA

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

The Far End Common Equipment Failure (FE-EQPT-NSA) condition occurs when a non-service-affecting equipment failure is detected on the far-end DS-3 equipment. The prefix FE occurs when the main alarm is occurring at the far-end 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.



Caution

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

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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.97 FE-FRCDWKSWPR-RING

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

The Far End Ring Working Facility Forced to Switch to Protection (FE-FRCDWKSWPR-RING) condition occurs from a far-end node when a ring is forced from working to protect using the FORCE RING command.

The prefix FE means the main alarm is occurring at the far-end 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. See the [“Clear a BLSR External Switching Command” procedure on page 2-215](#) for instructions.
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.98 FE-FRCDWKSWPR-SPAN

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

The Far End Working Facility Forced to Switch to Protection Span (FE-FRCDWKSWPR-SPAN) condition occurs from a far-end 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 far-end 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. See the [“Clear a BLSR External Switching Command” procedure on page 2-215](#) for instructions.
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.99 FE-IDLE

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

The Far End Idle (FE-IDLE) condition occurs when a far-end node detects an idle DS-3 signal.

The prefix FE in an alarm or condition occurs when the main alarm is occurring at the far-end 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. Complete the [“Clear a BLSR External Switching Command” procedure on page 2-215](#).
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.100 FE-LOCKOUTOFPR-SPAN

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

The Far-End Lock Out of Protection Span (FE-LOCKOUTOFPR-SPAN) condition occurs when a BSLR span is locked out of the protection system from a far-end node using the Lockout Protect Span command.

The prefix FE means the main alarm is occurring at the far-end 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. See the “[Clear a BLSR External Switching Command](#)” procedure on [page 2-215](#) for instructions.
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.101 FE-LOF

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

The Far End LOF (FE-LOF) condition occurs when a far-end node reports the “[LOF \(DS3\)](#)” alarm on [page 2-122](#).

The prefix FE in an alarm or condition occurs when the main alarm is occurring at the far-end 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 2-121](#). It also applies to FE-LOF.
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.102 FE-LOS

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

The Far End LOS (FE-LOS) condition occurs when a far-end node reports the “[LOS \(DS3\) alarm on page 2-129](#)”.

The prefix FE occurs when the main alarm is occurring at the far-end 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 2-128.
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.103 FE-MANWKSWPR-RING

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

The Far End Ring Manual Switch of Working Facility to Protect (FEMANWKSWPR-RING) condition occurs when a BLSR working ring is switched from working to protect at a far-end node using the MANUAL RING command.

The prefix FE means the main alarm is occurring at the far-end 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 2-215.
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.104 FE-MANWKSWPR-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: OCN

The Far-End Span Manual Switch Working Facility to Protect (FE-MANWKSWPR-SPAN) condition occurs when a BLSR span is switched from working to protect at the far-end node using the MANUAL SPAN command.

The prefix FE means the main alarm is occurring at the far-end 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” procedure on page 2-215](#).
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.105 FEPRLF

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

The Far End Protection Line Failure (FEPRLF) alarm occurs when an APS channel [“SF \(DS1, DS3\)” condition on page 2-182](#) occurs on the protect card coming into the node.

**Note**

The FEPRLF alarm occurs only on the ONS 15454 when bidirectional protection is used on optical (traffic) 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 condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.106 FIBERTEMP-DEG

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

The Fiber Temperature Degrade (FIBERTEMP-DEG) 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 Card](#)” procedure on page 2-219 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).
-

2.7.107 FORCED-REQ

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

The Force Switch Request (FORCED-REQ) condition occurs when you enter the Force command on a span or card to force traffic from a working card or working span to a protection card 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 BLSR External Switching Command](#)” procedure on page 2-215.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.108 FORCED-REQ-RING

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

The Force Switch Request Ring (FORCED-REQ-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 2-215.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.109 FORCED-REQ-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The Force Switch Request Span (FORCED-REQ-SPAN) condition applies to optical trunk cards in 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 2-215.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.110 FRCDSWTOINT

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

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



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

2.7.111 FRCDSWTOPRI

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

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



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

2.7.112 FRCDSWTOSEC

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

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



Note

FRCDSWTOSEC is an informational condition. It does not require troubleshooting.

2.7.113 FRCDSWTOTHIRD

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

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



Note

FRCDSWTOTHIRD is an informational condition. It does not require troubleshooting.

2.7.114 FRNGSYNC

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

The Free Running Synchronization Mode (FRNGSYNC) alarm 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 ONS 15454 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 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 Alarm

-
- 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 *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 2-195 and the “[SYNCSEC](#)” alarm on page 2-196.
- 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).
-

2.7.115 FSTSYNC

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

A Fast Start Synchronization Mode (FSTSYNC) alarm occurs when the ONS 15454 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 onto <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.

2.7.116 FULLPASSTHR-BI

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

The Bidirectional Full Pass-Through Active (FULLPASSTHR-BI) 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 2-215](#).
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.117 GAIN-HDEG

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

The Optical Amplifier Gain Degrade High (GAIN-HDEG) alarm is raised by OPT-BST amplifier cards on the Line-3 TX port and OPT-PRE cards on the Line-1 TX port when an internal problem in the card keeps the gain level from maintaining the set-point.

Clear the GAIN-HDEG Alarm

-
- Step 1** This alarm does not immediately affect traffic, but eventually to clear the alarm you will need to complete the [“Physically Replace a Card” procedure on page 2-219](#).

**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. Refer to the *Cisco ONS 15454 Procedure Guide* for information.

**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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.118 GAIN-HFAIL

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

The Optical Amplifier Gain High Fail (GAIN-HFAIL) alarm is raised by OPT-BST amplifier cards on the Line-3 TX port and OPT-PRE cards on the Line-1 TX port when an internal problem causes the card to fail by forcing the gain level to consistently exceed the set-point.

Clear the GAIN-HFAIL Alarm

Step 1 Complete the [“Physically Replace a Card” procedure on page 2-219](#).

**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. Refer to the *Cisco ONS 15454 Procedure Guide* for information.

**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 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.

2.7.119 GAIN-LDEG

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

The Optical Amplifier Gain Degradate Low (GAIN-LDEG) alarm is raised by OPT-BST amplifier cards on the Line-3 TX port and OPT-PRE cards on the Line-1 TX port when an internal problem in the card keeps the gain level from reaching the set-point.

Clear the GAIN-LDEG Alarm

Step 1 This alarm does not immediately affect traffic. But eventually, to clear the alarm, you will need to complete the [“Physically Replace a Card” procedure on page 2-219](#).



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. Refer to the *Cisco ONS 15454 Procedure Guide* for information.



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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.120 GAIN-LFAIL

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

The Optical Amplifier Gain Fail Low (GAIN-LFAIL) alarm is raised by OPT-BST amplifier cards on the Line-3 TX port and OPT-PRE cards on the Line-1 TX port when an internal problem in the card causes the card to fail by preventing the gain level from reaching the set-point.

Clear the GAIN-LFAIL Alarm

Step 1 Complete the [“Physically Replace a Card” procedure on page 2-219](#).



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. Refer to the *Cisco ONS 15454 Procedure Guide* for information.



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 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.
-

2.7.121 GCC-EOC

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Gnu C Compiler (GCC) Embedded Operation Channel Failure (GCC-EOC) alarm applies to the optical transport network (OTN) communication channel for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or 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 2-67.
- Step 2** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.122 GE-OOSYNC

- Critical (CR), Service-Affecting (SA)
- Logical Objects: CLIENT, TRUNK

The Gigabit Ethernet Out of Synchronization (GE-OOSYNC) alarm applies to TXP_MR_10G, TXP_MR_2.5G, or 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, 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 it 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 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.
-

2.7.123 HIBATVG

- Major (MJ), Service-Affecting (SA)

- Logical Object: PWR

The High Voltage Battery (HI-BATVG) alarm occurs in a –48 VDC environment when a battery lead's 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*.)

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 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.
-

2.7.124 HI-LASERBIAS

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

The Equipment High Transmit Laser Bias Current (HI-LASERBIAS) alarm is raised against TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or 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's 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's 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 2-117. 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 “[Switch Protection Group Traffic with an External Switching Command](#)” procedure on page 2-216 for information.



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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.125 HI-RXPOWER

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

The Equipment High Receive Power (HI-RXPOWER) 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, 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. The 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 dense wavelength division multiplexing 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 once and data alarms would be present. If wavelengths are drifting, the data is garbled and receive power increases by about +3 dB.

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 [“Perform a Facility \(Line\) Loopback on a Source DS-N Port \(West to East\)”](#) procedure on page 1-8.

Step 7 If a port is bad and you need to use all the port bandwidth, complete the [“Physically Replace a Card”](#) procedure on page 2-219. 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 [“Switch Protection Group Traffic with an External Switching Command”](#) procedure on page 2-216 for more information.



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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.126 HITEMP

- Critical (CR), Service-Affecting (SA) for NE
- Minor (MN), Non-Service Affecting (NSA) for EQPT
- Logical Objects: EQPT, NE

The High Temperature (HITEMP) alarm occurs when the temperature of the ONS 15454 is above 122 degrees F (50 degrees C).



Caution

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

Clear the HITEMP Alarm

- Step 1** View the temperature displayed on the ONS 15454 LCD front panel ([Figure 2-1 on page 2-35](#)).
- 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.
- Step 4** If airflow is not blocked, physically ensure that blank faceplates fill the ONS 15454 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 3-5](#).
- Step 6** If the filter is clean, complete the [“Remove and Reinsert Fan-Tray Assembly” procedure on page 2-220](#).



Note The fan should run immediately when correctly inserted.

- Step 7** If the fan does not run or the alarm persists, complete the [“Replace the Fan-Tray Assembly” procedure on page 3-10](#).
- Step 8** If the replacement fan-tray assembly does not operate correctly, log onto <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.
-

2.7.127 HI-TXPOWER

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

The Equipment High Transmit Power (HI-TXPOWER) alarm is an indicator on the 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_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 TX Power 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 Card” procedure on page 2-219](#).



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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.



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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.128 HLDOVRSYNC

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

The Holdover Synchronization Mode (HLDOVRSYNC) alarm 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 alarm indicates that the ONS 15454 has gone into holdover and is using the ONS 15454 internal reference clock, which is a Stratum 3-level timing device. The alarm clears when primary or secondary timing is reestablished.

Clear the HLDOVRSYNC Alarm

-
- Step 1** Clear additional alarms that relate to timing, such as:
- [FRNGSYNC, page 2-96](#)
 - [FSTSYNC, page 2-97](#)
 - [HLDOVRSYNC, page 2-104](#)
 - [LOF \(BITS\), page 2-120](#)

- [LOS \(BITS\)](#), page 2-127
- [MANSWTOINT](#), page 2-146
- [MANSWTOPRI](#), page 2-146
- [MANSWTOSEC](#), page 2-146
- [MANSWTOTHIRD](#), page 2-147
- [SWTOPRI](#), page 2-194
- [SWTOSEC](#), page 2-194
- [SWTOTHIRD](#), page 2-194
- [SYNC-FREQ](#), page 2-195
- [SYNCPRI](#), page 2-195
- [SYNCSEC](#), page 2-196
- [SYNCTHIRD](#), page 2-197

Step 2 Reestablish a primary and secondary timing source according to local site practice.

Step 3 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.

2.7.129 I-HITEMP

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

The Industrial High Temperature (I-HITEMP) 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 2-103.

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.

2.7.130 IMPROPRMVL

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

The Improper Removal (IMPROPRMVL) 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.

**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.

**Caution**

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

**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 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):

**Caution**

Before placing a port out of service (OOS), ensure that no live traffic is present.

- a. In node view, double-click the reporting card to display the card view.
- b. Click the **Provisioning > Line** tab.
- c. Click the **State** column of any in-service (IS) ports.
- d. Choose **OOS** 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 2-217](#).

**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 **Provisioning > DCC/GCC/OSC** 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 pull-down menu 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 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.
-

2.7.131 INC-GFP-OUTOFFRAME

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FCMR

The Out of Frame Detected by general framing procedure (GFP) Receiver condition (INC-GFP-OUTOFFRAME) can be caused by anything that prevents GFP communication across the SONET link, such as typical errors (AIS-P, LOP-P, PLM-P, or UNEQ-P); virtual concatenation (VCAT) member errors (SQM); and VCAT group errors. If a VCAT is present, the VCG-DOWN, LOA, or LOM alarms are generated if any of the normal SONET errors are generated.

Clear the INC-GFP-OUTOFFRAME Condition

- Step 1** Resolve any normal SONET errors also occurring on the errored circuit. Refer to the appropriate sections for any alarms that are present:
- [“AIS-P” alarm on page 2-22](#)
 - [“LOP-P” alarm on page 2-125](#)
 - [“PLM-P” alarm on page 2-167](#)
 - [“UNEQ-P” alarm on page 2-204](#)
-
- Step 1** If the errored circuit is a VCAT circuit and no other SONET alarms are occurring, look for and clear any VCAT alarms. Refer to the appropriate sections for any alarms that are present:
- [“SQM” alarm on page 2-188](#)
 - [“VCG-DEG” alarm on page 2-206](#)

- “VCG-DOWN” alarm on page 2-207.

- Step 2** If a protection switch occurred on the STS carrying the circuit, the INC-GFP-OUTOFFRAME condition will clear when the working circuit is restored and able to carry traffic. For general information about protection switches, refer to the *Cisco ONS 15454 Procedure Guide* and the *Cisco ONS 15454 Reference Manual*. To clear a protection switch (if the working card or port is available for service), complete the “Clear a Protection Group External Switching Command” procedure on page 2-216.
- 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).
-

2.7.132 INC-GFP-SIGLOSS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FCMR

The Client Signal Loss Frames Detected by GFP Server (INC-GFP-SIGLOSS) condition occurs when the upstream GFP transmitter has no signal from its fibre channel link. This condition occurs in conjunction with the “INC-SIGLOSS” alarm on page 2-109.

Clear the INC-GFP-SIGLOSS Condition

- Step 1** Check the fibre channel data port connection at the remote fibre channel card port on the other end of the SONET link.
- Step 2** Verify fiber continuity to the port.
- 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 condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-


2.7.133 INC-GFP-SYNCLOSS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: FCMR

The Client Synchronization Loss Frames Detected by GFP Receiver (INC-GFP-SYNCLOSS) condition occurs when the upstream GFP transmitter has no synchronization from its fibre channel link. This alarm is raised in conjunction with the “INC-SYNCLOSS” alarm on page 2-110.

Errors in synchronization can be caused if the fibre channel link is set for a speed that is not compatible with the attached equipment or if the port has an GBIC connector that is incompatible with the link speed. When the GBIC does not support the line speed, the PORT-MISMATCH alarm could also be raised.

Clear the INC-GFP-SYNCLOSS Condition

-
- Step 1** For the errored circuit, log into both ends of the SONET link where the fibre channel connection is present, and ensure that the fibre channel link is set to run at a compatible speed for the attached equipment (for example, 1 Gbps or 2 Gbps):
- Double-click the fibre channel card to display the card view.
 - Click the **Provisioning > Port** tabs.
 - Under the Port Rate column, choose a speed that is compatible with the attached fibre channel equipment (either 1 Gbps or 2 Gbps).
-  **Note** You must choose the same line rate on both ends of the fibre channel link.
- Click **Apply**.
- Step 2** If the line rate is correctly set on both ends of the circuit, the remote card could have an incompatible GBIC for the link speed.
- 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).
-

2.7.134 INC-ISD

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

The DS-3 Idle (INC-ISD) 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 OO-MT state. It is resolved when the OOS state ends.



Note INC-ISD is a condition and not an alarm. It is for information only and does not require troubleshooting.

2.7.135 INC-SIGLOSS

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: FCMR

The Incoming Signal Loss on the Fibre Channel Interface (INC-SIGLOSS) alarm is raised when there is a signal loss at the local fibre channel port. (The “[INC-GFP-SIGLOSS](#)” alarm on page 2-108 is raised at the far-end port in conjunction with this alarm.)

Clear the INC-SIGLOSS Alarm

-
- Step 1** Check the fibre channel data port connection at the near-end fibre channel card port of the SONET link.
- Step 2** Verify fiber continuity to the port.

- 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).
-

2.7.136 INC-SYNCLOSS

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: FCMR

The Incoming Synchronization Loss on the Fibre Channel Interface (INC-SYNCLOSS) alarm is raised when there is a synchronization error at the local fibre channel port. (The [“INC-GFP-SYNCLOSS” alarm on page 2-108](#) is raised at the far-end port in conjunction with this alarm.)

Clear the INC-SYNCLOSS Alarm

- Step 1** Complete the [“Clear the INC-GFP-SYNCLOSS Condition” procedure on page 2-109](#).
- Step 2** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.137 INHSWPR

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

The Inhibit Switch To Protect Request on Equipment (INHSWPR) 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** Complete the [“Clear a Protection Group External Switching Command” procedure on page 2-216](#).
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.138 INHSWWKG

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

The Inhibit Switch To Working Request on Equipment (INHSWWKG) 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** Complete the “[Clear a Protection Group External Switching Command](#)” procedure on page 2-216.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.139 INTRUSION-PSWD

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

The Security Intrusion Incorrect Password (INTRUSION-PSWD) condition occurs after a user attempts a settable (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. This condition is only shown in Superuser login sessions, not login sessions for lower-level users. The INTRUSION-PSWD condition is automatically cleared when a settable lockout timeout expires, or it can be manually cleared in CTC by the Superuser if lockout is permanent.

Clear the INTRUSION-PSWD Condition

-
- Step 1** In node view, click the **Provisioning > Security** tabs.
- Step 2** Click the **Clear Security Intrusion Password Alarm** button.
- 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).
-

2.7.140 INVMACADR

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: AIP

The Equipment Failure Invalid MAC Address (INVMACADR) alarm occurs when the ONS 15454 Media Access Control layer address (MAC address) is invalid. Each ONS 15454 has a unique, permanently assigned MAC address that resides on an Alarm Interface Panel (AIP) EEPROM. The TCC2 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 the Cisco Transport Controller (CTC).

The Cisco ONS 15454 uses both IP and MAC addresses for circuit routing. When an INVMACADR alarm exists on a node, you will see an incomplete circuit in the CTC circuit status column. The circuit works and is able to carry traffic, but CTC cannot logically display the circuit's 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 uses the default MAC address (00-10-cf-ff-ff-ff).
- There is a read error occurring on one of the redundant TCC2 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 and resolve them.
- Step 2** Determine whether the LCD display on the fan tray is blank or if the text is garbled. If so, proceed to [Step 8 \(Figure 2-1 on page 2-35\)](#). If not, continue with Step 3.
- Step 3** At the earliest maintenance window, reset the standby TCC2:



Note The reset will take 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 card.
If you are looking at the physical ONS 15454, the ACT/SBY LED of the active TCC2 is green. The ACT/STBLY LED of the standby TCC2 is amber.
 - c. Right-click the standby TCC2 card in CTC.
 - d. Choose **Reset Card** from the shortcut menu.
 - e. Click **Yes** at 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. For LED appearance, see the [“Non-DWDM Card LED State After Successful Reset”](#) section on [page 2-213](#).
 - g. Double-click the node and ensure that the reset TCC2 card is still in standby mode and that the other TCC2 card is active.
If you are looking at the physical ONS 15454, the ACT/SBY LED of the active TCC2 is green. The ACT/STBLY LED of the standby TCC2 is amber.
 - h. Ensure that no new alarms appear in the Alarms window in CTC that are associated with this reset.
- If the standby TCC2 fails to boot into standby mode and reloads continuously, the alarm interface panel (AIP) is likely defective. In this case, the standby TCC2 is unsuccessfully attempting to read the EEPROM located on the AIP. The TCC2 reloads until it reads the EEPROM. Proceed to [Step 8](#).

- Step 4** If the standby TCC2 rebooted successfully into standby mode, complete the [“Reset Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#).
- Resetting the active TCC2 causes the standby TCC2 to become active. The standby TCC2 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 Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#) again to place the standby TCC2 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 resets, this indicates that the AIP is probably defective. Proceed to [Step 8](#).
- If the INVMACADR was raised during one TCC2 reset and cleared during the other, the TCC2 that was active during the alarm raise needs to be replaced. Continue with [Step 7](#).
- Step 7** If the faulty TCC2 is currently in standby mode, complete the [“Physically Replace a Card” procedure on page 2-219](#) for this card. If the faulty TCC2 card is currently active, during the next available maintenance window complete the [“Reset Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#) and then complete the [“Physically Replace a Card” procedure on page 2-219](#).
-
-  **Note** If the replacement TCC2 is loaded with a different software version from the current TCC2 card, the card bootup may take up to 30 minutes. During this time, the card LEDs flicker between Fail and Act/Sby as the active TCC2 version software is copied to the new standby card.
-
- Step 8** Open a case with the Cisco Technical Assistance Center (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 3-12](#).
- Step 11** If the alarm does not clear, log onto <http://www.cisco.com/tac> for more information or call TAC (1 800 553-2447).
-

2.7.141 IOSCFGCOPY

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

The IOS Configuration Copy in Progress (IOSCFGCOPY) condition occurs on ML-Series Ethernet cards when an 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 2-183](#) but it applies to ML-Series Ethernet cards rather than to the TCC2.)

The condition clears after the copy operation is complete. (If it does not complete correctly, the [“NO-CONFIG” condition on page 2-152](#) could be raised.)



Note IOSCFGCOPY is an informational condition.

2.7.142 KB-PASSTHR

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

The K Bytes Pass Through Active (KB-PASSTHR) 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.

Clear the KB-PASSTHR Condition

-
- Step 1** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-215.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.143 KBYTE-APS-CHANNEL-FAILURE

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

The APS Channel Failure (KBYTE-APS-CHANNEL-FAILURE) alarm is raised when there a span 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 occurs 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 AIS-P, LOF, LOS, or SF-BER alarms.

Clear the KBYTE-APS-CHANNEL-FAILURE Alarm

-
- Step 1** The alarm most frequently is 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*.
- Step 2** If the error is not caused by misprovisioning, it is due to checksum errors within an OC-N, cross-connect, or TCC2 card. Complete the “[Side Switch the Active and Standby XC10G Cross-Connect cards](#)” alarm on page 2-216 to allow the 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.144 LAN-POL-REV

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

The LAN Connection Polarity Reversed (LAN-POL-REV) condition is not raised in shelves that contain TCC2 cards. It is raised by the TCC+ card during software upgrade when the card detects that a connected Ethernet cable has reversed receive wire pairs. The TCC+ 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*.
- 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).
-

2.7.145 LASER-APR

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Laser Auto Power Reduction (LASER-APR) condition occurs on DWDM amplifiers (OPT-BST and OPT-PRE) when the amplifier works at a reduced power level for a fixed period during the automatic restart. The condition raises and clears within about 10 seconds.



Note

LASER-APR is information condition only and does not require troubleshooting.

2.7.146 LASERBIAS-DEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OTS

The Laser Bias Degrade (LASERBIAS-DEG) alarm occurs on DWDM amplifiers (OPT-BST and OPT-PRE) and optical service channel cards (OSCM and OSC-CSM) if the card laser crosses the laser bias degrade threshold. This degradation occurs due to laser aging.

Clear the LASERBIAS-DEG Alarm

-
- Step 1** This alarm does not immediately affect traffic, but eventually to clear this alarm, complete the “[Physically Replace a Card](#)” procedure on page 2-219.



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. Refer to the *Cisco ONS 15454 Procedure Guide* for information.



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).

2.7.147 LASERBIAS-FAIL

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: AOTS

The Laser Bias Failure (LASERBIAS-FAIL) alarm occurs on DWDM amplifiers (OPT-BST and OPT-PRE) when a failure occurs on the card laser current control circuit, or if the laser is broken.

Clear the LASERBIAS-FAIL Alarm

Step 1 Complete the [“Physically Replace a Card” procedure on page 2-219](#) 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. Refer to the *Cisco ONS 15454 Procedure Guide* for information.



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).

2.7.148 LASEREOL

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

The Laser Approaching End of Life (LASEREOL) alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards. It is typically accompanied by the [“HI-LASERBIAS” alarm on page 2-101](#). It is an indicator that the laser in the card will need to 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 Card](#)” procedure on page 2-219.

**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 “[Switch Protection Group Traffic with an External Switching Command](#)” procedure on page 2-216 for more information.

**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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.149 LASERTEMP-DEG

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

The Laser Temperature Degrade (LASERTEMP-DEG) condition occurs on DWDM amplifiers (OPT-BST and OPT-PRE) when a failure occurs on the laser Peltier control circuit that degrades laser performance in the amplifier card.

Clear the LASERTEMP-DEG Alarm

Step 1 This alarm does not immediately affect traffic, but eventually to clear this alarm, complete the “[Physically Replace a Card](#)” procedure on page 2-219.

**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. Refer to the *Cisco ONS 15454 Procedure Guide* for information.

**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 condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.150 LKOUTPR-S

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

The Lockout of Protection Span (LKOUTPR-S) condition occurs on a BSLR node when traffic is locked out of a protect span using the Lockout Protect Span command.

Clear the LKOUTPR-S Condition

-
- Step 1** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-215.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.151 LKOUTWK-S (NA)

The LKOUTWK-S condition is not supported in this release. It is reserved for future development.

2.7.152 LMP-HELLODOWN

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: UCP-IPCC

The Link Management Protocol (LMP) Hello Down alarm (LMP-HELLODOWN) occurs when the Hello protocol, which monitors UCP control channel status, is not available for link management. The unavailability can be caused by physical layer errors (such as cabling) or by control channel misconfiguration.

Clear the LMP-HELLODOWN Alarm

-
- Step 1** Verify that transmit and receive cables are not crossed at each end (login site and neighbor site).
- Step 2** Verify that the “[LOF \(OCN\)](#)” alarm on page 2-123 is not present on the source or destination nodes. If so, complete the “[Clear the LOS \(OCN\) Alarm](#)” procedure on page 2-133.
- Step 3** If the alarm does not clear, complete the “[Clear the CKTDOWN Alarm](#)” procedure on page 2-51 to verify that IPCC provisioning is valid on both ends of the UNI.
- 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).
-

2.7.153 LMP-NDFAIL

- Minor (MN) Non-Service Affecting (NSA)

- Logical Object: UPC-IPCC

The LMP Neighbor Detection Fail (LMP-NDFAIL) alarm occurs when neighbor detection within the UCP has failed. LMP-NDFAIL can be caused by physical failure (such as cabling) between the neighbors or by control channel misconfiguration.

Clear the LMP-NDFAIL Alarm

-
- Step 1** Complete the “[Clear the LMP-HELLODOWN Alarm](#)” procedure on page 2-118.
- Step 2** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.154 LOA

- Critical (CR), Service-Affecting (SA)
- Logical Object: VCG

The Loss of Alignment (LOA) on a virtual concatenation group (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 2-217.
- Step 5** Recreate the circuit using the procedure in the *Cisco ONS 15454 Procedure Guide*.
- Step 6** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.7.155 LOCKOUT-REQ

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, EQPT, OCN, STSMON, TRUNK, VT-MON

The Lockout Switch Request on Facility or Equipment (LOCKOUT-REQ) condition occurs when a user initiates a lockout switch request for an OC-N card or a lockout switch request on a path protection at the path level. 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 Path Protection Lockout](#)” procedure on page 2-215.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.156 LOF (BITS)

- Major (MJ), Service-Affecting (SA)
- Logical Object: BITS

The Loss of Frame (LOF) BITS alarm occurs when a port on the TCC2 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.



Caution

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



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:
- In node view 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 pull-down menu.
 - 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 pull-down menu.



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, complete the [“Physically Replace a Card” procedure on page 2-219](#) for the TCC2 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 3 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.

2.7.157 LOF (CLIENT)

- Critical (CR), Service-Affecting (SA)
- Logical Object: CLIENT

The Loss of Frame for a DWDM client applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards. It is raised when the card port 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 (CLIENT) Alarm

Step 1 Complete the [“Clear the LOF \(OCN\) Alarm” procedure on page 2-124](#).

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.

2.7.158 LOF (DS1)

- 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 DS1-N-14 card, the transmitting equipment could have its framing set to a format that differs from the receiving ONS 15454.

Clear the LOF (DS1) Alarm

Step 1 Verify that the line framing and line coding match between the DS1-N-14 port and the signal source:

- a. In CTC, note the slot and port reporting the alarm.

- b. Find the coding and framing formats of the signal source for the card reporting the alarm. You may need to contact your network administrator for the format information.
- c. Display the card view of the reporting card.
- d. Click the **Provisioning > Line** tabs.
- e. 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 pull-down menu and choose the matching type.
- f. Verify that the reporting Line Coding matches the signal source's 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 right type from the pull-down menu.
- g. 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 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.

2.7.159 LOF (DS3)

- 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 ONS 15454. 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:
- a. Display the card view of the reporting card.
 - b. Click the **Provisioning > Line** tabs.
 - c. Verify that the line type of the reporting port matches the line type of the signal source.
 - d. If the signal source line type does not match the reporting port, click **Line Type** and choose **C Bit** from the pull-down menu.
 - e. Click **Apply**.

- Step 2** 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.
-

2.7.160 LOF (EC1-12)

- Critical (CR), Service-Affecting (SA)
- Logical Object: EC1-12

The EC1-12 LOF alarm occurs when a port on the reporting EC1-12 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.

**Caution**

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

Clear the LOF (EC1-12) Alarm

- Step 1** Verify cabling continuity to the port reporting the alarm.
- 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*.
- Step 3** If the alarm does not clear, see the “[Network Troubleshooting Tests](#)” section on page 1-2 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).
-

2.7.161 LOF (OCN)

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

The LOF alarm occurs when a port on the reporting OC-N, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G 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.

LOF on an OC-N card is sometimes an indication that the OC-N card reporting the alarm expects a specific line rate and the input line rate source does not match the input line rate of the optical receiver.

**Caution**

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

Clear the LOF (OCN) Alarm

-
- Step 1** Verify cabling continuity to the port reporting the alarm.
- 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*.
- Step 3** If the alarm does not clear, see the “[Network Troubleshooting Tests](#)” section on page 1-2 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).
-

2.7.162 LOF (TRUNK)

- 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, or 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 2-124.
- Step 2** 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.
-

2.7.163 LOM

- Critical (CR), Service-Affecting (SA)
- Logical Objects: STSTRM, TRUNK, VT-TERM

The optical transport unit (OTU) Loss of Multiframe (LOM) 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, 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 three milliseconds.

Clear the LOM Alarm

-
- Step 1** Complete the “[Clear the SD-L Condition](#)” procedure on page 2-180.

- Step 2** 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.
-

2.7.164 LOP-P

- Critical (CR), Service-Affecting (SA)
- Logical Objects: STSMON, STSTRM

A Loss of Pointer Path (LOP-P) 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.



Caution

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

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 STS 3c instead of an STS1, this will cause 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.
- 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 2-217](#).
- Step 5** Recreate the circuit for the correct size. For instructions, see the “Create Circuits and Tunnels” chapter in the *Cisco ONS 15454 Procedure Guide*.
- Step 6** 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.
-

2.7.165 LOP-V

- Major (MJ), Service-Affecting (SA)
- Logical Objects: VT-MON, VT-TERM

The LOP VT (LOP-V) 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.

**Caution**

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

Clear the LOP-V Alarm

-
- Step 1** Complete the “[Clear the LOP-P Alarm](#)” procedure on page 2-125.
- Step 2** 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.
-

2.7.166 LO-RXPOWER

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN

The Equipment Low Receive Power (LO-RXPOWER) alarm is an indicator for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or 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 dense wavelength division multiplexing 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*.
- 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 will not be as precise, but you will 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 “[Perform a Facility \(Line\) Loopback on a Source DS-N Port \(West to East\)](#)” procedure on page 1-8.
- Step 8** If a port is bad and you need to use all the port bandwidth, complete the “[Physically Replace a Card](#)” procedure on page 2-219. 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 “[Switch Protection Group Traffic with an External Switching Command](#)” procedure on page 2-216 for more information.

**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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.167 LOS (BITS)

- Major (MJ), Service-Affecting (SA)
- Logical Object: BITS

The LOS (BITS) alarm indicates that the TCC2 card has an LOS from the BITS timing source. The LOS (BITS-N) means the BITS clock or the connection to the BITS clock failed.

**Caution**

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

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.
- Step 2** If wiring is good, verify that the BITS clock is operating properly.
- Step 3** 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.

2.7.168 LOS (CLIENT)

- Critical (CR), Service-Affecting (SA)
- Logical Object: CLIENT

The Loss of Signal for a DWDM client applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards. The alarm is raised when the card port is not receiving input. An AIS is sent upstream.

**Note**

The alarm severity of the client-side Loss of Signal (LOS) alarm is based on the protection status of the card; a critical (CR) alarm is raised for a working card and a minor (MN) alarm is raised for a standby card. If a working card has an active LOS alarm, the alarm severity is CR even though the circuit is protected.

Clear the LOS (CLIENT) Alarm

-
- Step 1** Complete the “[Clear the LOS \(OCN\) Alarm](#)” procedure on page 2-133.
- Step 2** 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.
-

2.7.169 LOS (DS1)

- Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

A LOS (DS-1) 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.

**Caution**

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

Clear the LOS (DS1) Alarm

-
- Step 1** Verify that the fiber cable is properly connected and attached to the correct port.
If an optical TDM signal such as an OC-3 or OC-12 is plugged into an E1000-2 or G1000-4 card GBIC connector, this can trigger an LOS.
- 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. LOS can be caused by a non-assigned port placed in service (IS).
- Double-click the card to display the card view.
 - Click the **Maintenance > Loopback** tabs.
 - Look under the State column to determine the port’s status.
- Step 4** If the port is assigned, verify that the correct port is in service:
- To confirm this physically, confirm that the card shows a green LED on the physical card.
A green LED indicates an active card. An amber LED indicates a standby card.
 - To determine this virtually, double-click the card in CTC to display the card view.

- Click the **Provisioning > Line** tabs.
- Verify that the **State** column lists the port as IS.
- If the State column lists the port as OOS, 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.
- 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.
- 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 Card” procedure on page 2-219](#) 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.

**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 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.

2.7.170 LOS (DS3)

- Critical (CR), Service-Affecting (SA)
- Logical Object: DS3

The LOS (DS-3) 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.

**Caution**

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

**Note**

If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place. The circuit will be 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 2-128.
- Step 2** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.171 LOS (EC1-12)

- Critical (CR), Service-Affecting (SA)
- Logical Object: EC1-12

LOS on an EC1-12 port occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS (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.



Caution

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



Note

If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place. The circuit will be 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 (EC1-12) Alarm

-
- Step 1** Verify cabling continuity to the port reporting the alarm.
- Step 2** If the cabling is okay, verify that the correct port is in service:
- Confirm that the card shows a green LED in CTC or on the physical card.
A green LED indicates an active card. An amber 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 State column lists the port as IS.
 - If the State column lists the port as OOS, 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.
- 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 (EC1-12).

- 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 (EC1-12), or if clearing an alarm did not clear the LOS, complete the [“Physically Replace a Card” procedure on page 2-219](#) 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.

**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 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.

2.7.172 LOS (FUDC)

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: FUDC

The LOS on the F1 user data channel (FUDC) alarm is raised if there is a UDC circuit created on the AIC-I DCC port but the port is not receiving signal input. The downstream node will have an AIS condition raised against the AIC-I DCC port transmitting the UDC.

Clear the LOS (FUDC) Alarm

- Step 1** Verify cable continuity to the AIC-I UDC port.
- 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*.
- 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*.
 - 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 Card” procedure on page 2-219](#) 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.

**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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.173 LOS (MSUDC)

The LOS alarm for the MSUDC is not supported in this platform in this release. It is reserved for future development.

2.7.174 LOS (OCN)

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

A 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).

**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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.

**Caution**

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

**Note**

If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place. The circuit will be 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.
- Step 2** If the cabling is okay, verify that the correct port is in service:
- Confirm that the card shows a green LED in CTC or on the physical card.
A green LED indicates an active card. An amber 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 State column lists the port as IS.
 - If the State column lists the port as OOS, 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*.
- Step 4** If the alarm does not clear, verify that the power level of the optical signal is within the OC-N card's receiver specifications. The "[OC-N Card Transmit and Receive Levels](#)" section on page 1-102 lists these specifications for each OC-N card, and the *Cisco ONS 15454 Reference Manual* lists levels for DWDM cards.
- 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 (OC-N), or if clearing an alarm did not clear the LOS, complete the "[Physically Replace a Card](#)" procedure on page 2-219 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 "[Switch Protection Group Traffic with an External Switching Command](#)" procedure on page 2-216 for more information.

**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 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.
-

2.7.175 LOS (OTS)

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

The Loss of Signal for the optical transport section (OTS) applies to add/drop, amplifier, multiplexer, demultiplexer, and combiner cards. It indicates that there is a loss or received signal at the OSCM, OSC-CSM card or OPT-BST card port. Troubleshooting for this alarm is similar to [LOS \(OCN\)](#), page 2-132.

Clear the LOS (OTS) Alarm

- Step 1** Verify fiber continuity to the port.
- 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, Release 2.5*.)
- 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:
- In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.
 - Consult the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5* 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*.
- Step 7** If the transmitted power value is outside of the expected range, troubleshoot using the DWDM acceptance tests in the *Cisco ONS 15454 Procedure 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 Card” procedure on page 2-219](#) 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 [“Alarm Procedures” section on page 2-21](#) for commonly used lockout and traffic-switching procedures. For detailed information and guidelines for traffic switching, refer to the *Cisco ONS 15454 Procedure Guide*.

**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 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.

2.7.176 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.
- 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*.
- 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 *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 Card” procedure on page 2-219](#) 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 [“Verify or Create Node DCC Terminations” section on page 2-214](#) for commonly used 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.

2.7.177 LOS-P

- Default Severity: Critical (CR), Service-Affecting (SA)
- Logical Objects: CLIENT, TRUNK

The Path Loss of Signal (LOS-P) alarm applies to all input ports of AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, OPT-BST, 32MUX-O, 32DMX-O, and OSC-CSM cards when there is a loss of received signal at an input port caused by MXP or TXP transmit port errors.

Clear the LOS-P Alarm

- Step 1** Check the fiber cable connection between the MXP or TXP card and the DWDM card.
- Step 2** Verify that the MXP or TXP card TRUNK TX port is in IS state. If not, change the state to IS:
- Double-click the card to display the card view.
 - For the port, choose IS from the State column.

- Step 3** If port state is IS, check the output power on the transmit MXP or TXP card using CTC:
- On the transmitting node, double-click the card to display the card view.
 - Click the **Performance > Optics PM** tab.
 - Under the **Param** column, view the TX Optical Pwr value for the port.
- Step 4** Check this value against the TXP or MXP specifications.
- Step 5** If the value is within specifications, proceed to [Step 6](#). If the value is outside of specifications, complete the following steps to turn on the OCHN connection and clear the LOS-P alarm:
- If you are not already in card view for the alarmed card, double-click it to display the card view.
 - Click the **Provisioning > Optical Thresholds** tab.
 - Identify the provisioned **VOA Attenuation Reference** parameter.
 - Double-click **VOA Attenuation Calibration** and enter a value exactly opposite to the VOA attenuation reference value. For example, if the reference value is 20 dBm, set the calibration value at -20 dBm.
 - Click **Apply**.



Note This procedure only temporarily adjusts system optical performance. An out-of-specification TXP or MXP card must eventually be replaced to guarantee system optical performance.

- Step 6** If the alarm does not clear, look for any other upstream alarm that could be identified as the source of the problem.
- Step 7** If no other alarms that could be the source of the LOS-P exist, place all of the card ports in OOS state.
- Step 8** Complete the [“Physically Replace a Card” procedure on page 2-219](#) for the reporting card.



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 state.

- 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.
-

2.7.178 LO-TXPOWER

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

The Equipment Low Transmit Power (LO-TXPOWER) alarm is an indicator for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or 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 MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G 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 Card” procedure on page 2-219](#).

**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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.

**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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.179 LPBKCRS

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

The Loopback Cross-Connect (LPBKCRS) condition indicates that there is a software cross-connect loopback active between a traffic (optical) card and an XC10G cross-connect card. A cross-connect loopback test occurs below line speed and does not affect traffic.

For more information on loopbacks, see the [“Identify Points of Failure on a DS-N Circuit Path” section on page 1-8](#).

**Note**

XC 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 traffic (optical) card in CTC to display the card view.
- Step 2** Click the **Provisioning > SONET STS** tabs.
- Step 3** In the **XC Loopback** column, deselect the check box for the port.
- Step 4** Click **Apply**.
- Step 5** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.180 LPBKDS1FEAC

- 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 (LPBKDS1FEAC) on the DS3XM-6 card occurs when a DS-1 loopback signal is received from the far-end 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 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 pull-down menu.
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.181 LPBKDS1FEAC-CMD

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS1

The LPBKDS1FEAC Command Sent (LPBKDS1FEAC-CMD) condition occurs on the near-end node when you send a DS-1 FEAC loopback. For more information about FEAC loopbacks, see the [“Using the DS3XM-6 Card FEAC \(Loopback\) Functions”](#) section on page 1-35.



Note

LPBKDS1FEAC-CMD is an informational condition. It does not require troubleshooting.



Caution

CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

2.7.182 LPBKDS3FEAC

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

A Loopback Due to FEAC Command DS-3 (LPBKDS3FEAC) condition occurs when a DS3XM-6 or DS3-12E card loopback signal is received from the far-end node because of an FEAC command. An FEAC command is often used with loopbacks. LPBKDS3FEAC is only reported by DS3XM-6 cards and DS3-12E cards. A DS3XM-6 card both generates and reports 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. It 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 pull-down menu.
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.183 LPBKDS3FEAC-CMD

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

The LPBKDS3FEAC Command Sent (LPBKDS3FEAC-CMD) condition occurs on the near-end node when you send a DS-3 FEAC loopback. For more information about FEAC loopbacks, see the [“Using the DS3XM-6 Card FEAC \(Loopback\) Functions”](#) section on page 1-35.

**Note**

LPBKDS3FEAC-CMD is an informational condition. It does not require troubleshooting.

2.7.184 LPBKFACILITY (CLIENT, TRUNK)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

A Loopback Facility (LPBKFACILITY) condition on TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards occurs when a port has a software facility (line) loopback active.

For more information about loopbacks, see the [“Identify Points of Failure on a DS-N Circuit Path”](#) section on page 1-8.

**Caution**

CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (CLIENT, TRUNK) Condition

-
- Step 1** Complete the “[Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback](#)” procedure on page 2-217.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.185 LPBKFACILITY (DS1, DS3)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A LPBKFACILITY condition occurs when a software facility (line) loopback is active for a port on the reporting DS-1 or DS-3.

For more information about loopbacks, see the “[Network Troubleshooting Tests](#)” section on page 1-2 or the “[Identify Points of Failure on a DS-N Circuit Path](#)” section on page 1-8.

**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** In node view, double-click the reporting DS3XM-6 card to display the card view.
- Step 2** Click the **Maintenance > DS3** tab.
If the condition is reported against a DS-1 line, also click the **DS1** tab.
- Step 3** Complete the “[Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback](#)” procedure on page 2-217.
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.186 LPBKFACILITY (EC1-12)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: EC1-12

A LPBKFACILITY condition occurs when a software facility (line) loopback is active for a port on the reporting EC1-12 card.

For more information about loopbacks, see the [“Identify Points of Failure on a DS-N Circuit Path” section on page 1-8](#).



Caution

CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (EC1-12) Condition

-
- Step 1** The loopback originates from the DS3XM-6 card. Complete the [“Clear the LPBKDS3FEAC Condition” procedure on page 2-140](#).
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.187 LPBKFACILITY (G1000)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: G1000

A LPBKFACILITY condition occurs when a software facility (line) loopback is active for a port on the reporting G1000 Ethernet card.

For more information about loopbacks, see the [“Identify Points of Failure on a DS-N Circuit Path” section on page 1-8](#).



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 a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback” procedure on page 2-217](#).
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.188 LPBKFACILITY (OCN)

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

A LPBKFACILITY condition occurs when a software facility (line) loopback is active for a port on the reporting OC-N card.

For more information about loopbacks, see the [“Identify Points of Failure on a DS-N Circuit Path” section on page 1-8](#).

**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 a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback” procedure on page 2-217](#).
- Step 2** If the condition does not clear, log onto <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 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.

2.7.189 LPBKTERMINAL (CLIENT, TRUNK)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

A Loopback Terminal (LPBKTERMINAL) condition occurs when a software terminal (inward) loopback is active for a TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card port.

For more information about loopbacks, see the [“Identify Points of Failure on a DS-N Circuit Path” section on page 1-8](#).

**Caution**

CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKTERMINAL (CLIENT) Condition

- Step 1** Complete the [“Clear the LPBKFACILITY \(CLIENT, TRUNK\) Condition” procedure on page 2-141](#).
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.190 LPBKTERMINAL (DS1, DS3, EC-1-12, OCN)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3, EC1-12, OCN

A LPBKTERMINAL condition occurs when a software terminal (inward) loopback is active for a port on the reporting card. DS-N and OC-N terminal loopbacks do not typically return an AIS.


Note

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


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 more information about loopbacks, see the [“Network Troubleshooting Tests”](#) section on page 1-2.

Clear the LPBKTERMINAL (DS1, DS3, EC1-12, OCN) Condition

- Step 1** Complete the [“Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback”](#) procedure on page 2-217.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).


Note

Terminal (inward) loopback is not supported at the DS-1 level for the DS3XM-6 card.

2.7.191 LPBKTERMINAL (G1000)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: G1000

A LPBKTERMINAL condition occurs when a software terminal (inward) loopback is active for a port on the reporting G-1000 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 loopbacks, see the [“Network Troubleshooting Tests”](#) section on page 1-2.


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 a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback](#)” procedure on page 2-217.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.192 LWBATVG

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

The Low Voltage Battery (LWBATVG) alarm occurs in a –48 VDC environment when a battery lead’s 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*.)

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 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.
-

2.7.193 MAN-REQ

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

The Manual Switch Request (MAN-REQ) condition occurs when a user initiates a Manual switch request on an OC-N card or path protection path. Clearing the Manual switch clears the MAN-REQ condition.

Clear the MAN-REQ Condition

-
- Step 1** Complete the “[Clear a BLSR External Switching Command](#)” procedure on page 2-215.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.194 MANRESET

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

A User-Initiated Manual Reset (MAN-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. It does not require troubleshooting.

2.7.195 MANSWTOINT

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

The Manual Switch To Internal Clock (MANSWTOINT) condition occurs when the NE timing source is manually switched to the internal timing source.



Note

MANSWTOINT is an informational condition. It does not require troubleshooting.

2.7.196 MANSWTOPRI

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

The Manual Switch To Primary Reference (MANSWTOPRI) condition occurs when the NE timing source is manually switched to the primary timing source.



Note

MANSWTOPRI is an informational condition. It does not require troubleshooting.

2.7.197 MANSWTOSEC

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

The Manual Switch To Second Reference (MANSWTOSEC) condition occurs when the NE timing source is manually switched to the second timing source.



Note

MANSWTOSEC is an informational condition. It does not require troubleshooting.

2.7.198 MANSWTOTHIRD

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

The Manual Switch To Third Reference (MANSWTOTHIRD) condition occurs when the NE timing source is manually switched to the tertiary timing source.



Note

MANSWTOTHIRD is an informational condition. It does not require troubleshooting.

2.7.199 MANUAL-REQ-RING

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

The Manual Switch Request on Ring (MANUAL-REQ-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 2-215.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.200 MANUAL-REQ-SPAN

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, OCN, TRUNK

The Manual Switch Request on Span (MANUAL-REQ-SPAN) condition occurs on four-fiber 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 2-215.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.201 MEA (AIP)

- Critical (CR), Service-Affecting (SA)
- Logical Object: AIP

If the Mismatch of Equipment Attributes (MEA) alarm is reported against the Alarm Interface Panel (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 3-12](#).
- Step 2** 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.
-

2.7.202 MEA (EQPT)

- 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 (traffic) 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.



Note When a failed member of an XC pair is field-replaced with an XCVT card, the [“CTNEQPT-MISMATCH” alarm on page 2-58](#) is raised rather than the MEA alarm.

Clear the MEA (EQPT) Alarm

-
- Step 1** 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. 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, then 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.



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 2 Physically 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's faceplate.

- a. 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 3](#).
- b. 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 (traffic) card is incompatible and must be removed.



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.

- c. 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 XC10G, OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), proceed to [Step 3](#).
- d. 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 XC10G, 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.

Step 3 In CTC, click the **Inventory** tab to reveal the provisioned card type.

Step 4 If you prefer the card type depicted by CTC, complete the [“Physically Replace a Card” procedure on page 2-219](#) 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.



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 and 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):



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 **State** of any in-service ports.
- d. Choose **OOS** 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 2-217](#).



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 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.

2.7.203 MEA (FAN)

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

The MEA fan 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 ONS 15454 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.

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 3-10.
- 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 3-10.
- 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.
-

2.7.204 MEM-GONE

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

The Memory Gone (MEM-GONE) alarm occurs when data generated by software operations exceeds the memory capacity of the TCC2 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.205 MEM-LOW

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

The Free Memory of Card Almost Gone (MEM-LOW) alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC2 card. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the TCC2 card is exceeded, CTC ceases to function.

**Note**

The alarm does not require user intervention. If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.206 MFGMEM (AICI-AEP, AICI-AIE, BPLANE, FAN)

- Critical (CR), Service-Affecting (SA)
- Logical Objects: AICI-AEP, AICI-AIE, BPLANE, FAN

The Manufacturing Data Memory Failure (MFGMEM) alarm occurs if the ONS 15454 cannot access the data in the electronically erasable programmable read-only memory (EEPROM). Either the memory module on the component failed or the TCC2 lost the ability to read that module. The EEPROM stores manufacturing data that is needed for both compatibility and inventory issues. The EEPROM on the alarm interface panel (AIP) also stores the MAC address. An inability to read a valid MAC address disrupts IP connectivity and grays out the ONS 15454 icon on the CTC network view.

Clear the MFGMEM (AICI-AEP, AIE, BPLANE, FAN) Alarm

-
- Step 1** Complete the [“Reset Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#).
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 reseal the card, complete the [“Remove and Reinsert \(Reseat\) the Standby TCC2” procedure on page 2-218](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-219](#).
- Step 3** If the MFGMEM alarm continues to report after replacing the TCC2 cards, 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 3-10](#).
- Step 5** If the MFGMEM is reported from the AIP, the backplane, or the alarm persists after the fan-tray assembly is replaced, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.7.207 NO-CONFIG

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

The No Startup Configuration (NO-CONFIG) condition applies to ML-Series Ethernet (traffic) cards and occurs when you preprovision Slots 5 to 6 and 12 to 13 for the card without inserting the card first, or when you insert a card without preprovisioning. (This is an exception to the usual rule in card provisioning.) Because this is normal operation, you should expect this alarm during provisioning. When the startup configuration file is copied to the active TCC2, the alarm clears.

Clear the NO-CONFIG Condition

-
- Step 1** Create a startup configuration for the card in IOS.
Follow the card provisioning instructions in the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide*.
- Step 2** Upload the configuration file to the TCC2:
- 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 2-218](#).
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.208 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 2-111](#) 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.

2.7.209 NTWTPINC

The NTWTPINC condition is not used in this platform in this release. It is reserved for future development.

2.7.210 OCHNC-ACTIV-FAIL

The OCHNC-ACTIV-FAIL alarm is not used in this platform in this release. It is reserved for future development.

2.7.211 OCHNC-DEACTIV-FAIL

The OCHNC-DEACTIV-FAIL alarm is not used in this platform in this release. It is reserved for future development.

2.7.212 OCHNC-FAIL

The OCHNC-FAIL alarm is not used in this platform in this release. It is reserved for future development.

2.7.213 OCHNC-INC

The OCHNC-INC alarm is not used in this platform in this release. It is reserved for future development.

2.7.214 ODUK-AIS-PM

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Optical Data Unit (ODUK) AIS Path Monitoring (PM) condition (ODUK-AIS-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 for the cards. ODUK-AIS-PM is a secondary condition that indicates a more serious condition such as the [“LOS \(OCN\)” alarm on page 2-132](#) 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 [“ODUK-OCI-PM” condition on page 2-155](#).

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*.

Clear the ODUK-AIS-PM Condition

-
- Step 1** Determine whether upstream nodes and equipment have alarms, especially the [“LOS \(OCN\)” alarm on page 2-132](#), 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.215 ODUK-BDI-PM

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Backward Defect Indicator (BDI) PM condition (ODUK-BDI-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 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. ODUK-BDI-PM occurs when the [“PORT-CODE-MISM” condition on page 2-168](#) occurs upstream.

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*.

Clear the ODUK-BDI-PM Condition

-
- Step 1** Complete the [“Clear the OTUK-BDI Condition” procedure on page 2-162](#).
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.216 ODUK-LCK-PM

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Locked Defect (LCK) PM condition (ODUK-LCK-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 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 and MXP_2.5G_10G cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the ODUK-LCK-PM Condition

-
- | | |
|---------------|--|
| Step 1 | Unlock the upstream node signal. |
| Step 2 | If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447). |
-

2.7.217 ODUK-OCI-PM

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Open Connection Indication (OCI) PM condition (ODUK-OCI-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 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 “[ODUK-LCK-PM](#)” condition on [page 2-155](#) 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*.

Clear the ODUK-OCI-PM Condition

-
- | | |
|---------------|--|
| Step 1 | Verify the fiber connectivity at nodes upstream. |
| Step 2 | If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447). |
-

2.7.218 ODUK-SD-PM

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Signal Degrade (SD) 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-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*.

Clear the ODUK-SD-PM Condition

-
- Step 1** Complete the “[Clear the SD-L Condition](#)” procedure on page 2-180.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.219 ODUK-SF-PM

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The ODUK Signal Fail (SF) PM condition (ODUK-SF-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*.

Clear the ODUK-SF-PM Condition

-
- Step 1** Complete the “[Clear the SF \(DS1, DS3\) Condition](#)” procedure on page 2-182.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.220 ODUK-TIM-PM

- Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Object: TRUNK

The ODUK Trace Identifier Mismatch (TIM) PM condition (ODUK-TIM-PM) applies to the path monitoring area of the OTN overhead for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards. The condition occurs when there is a trace identifier mismatch in the data stream. ODUK-TIM-PM causes a “[ODUK-BDI-PM](#)” condition on page 2-154 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*.

Clear the ODUK-TIM-PM Condition

-
- Step 1** Complete the “[Clear the TIM-P Alarm](#)” procedure on page 2-199.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.221 OOU-TPT

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

The Out of Use Transport Failure (OOU-TPT) 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. It occurs in conjunction with the “[VCG-DEG](#)” alarm on page 2-206.

Clear the OOU-TPT Condition

-
- Step 1** Complete the “[Clear the VCG-DEG Condition](#)” procedure on page 2-207. Clearing that condition clears this condition as well.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.222 OPTNTWMIS

- Major (MJ), Non-Service Affecting (NSA)
- Logical Object: NE

The Optical Network Type Mismatch (OPNTWMIS) alarm is raised when DWDM nodes are not configured for the same type of network, either MetroCore and MetroAccess. All DWDM nodes on the same network must be configured for the same network type because automatic power control (APC) and automatic node setup (ANS) behave differently on each of these network types.

When the OPTNTWMIS occurs, the “APC-DISABLED” alarm on page 2-24 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.223 OPWR-HDEG

- 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, and 32MUX-O 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, and 32MUX-O OCH ports and OSC-CSM and OSCM OSC-TX ports, OPWR-HDEG indicates that the card has a variable optical attenuator (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.
- 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, Release 2.5* and decide what value to use for modifying the value:
- 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 Provisioning > Optical Chn > Optics Thresholds tab
- 32MUX Provisioning > Optical Chn > Optics Thresholds tab
- OSCM Provisioning > Optical Line > Optics Thresholds tab

- Step 5** If the received optical power level is within specifications, consult the *Cisco MetroPlanner DWDM Operations Guide, Release 2.5* 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, choose **IS** from the state drop-down list.

- Step 7** If the port is in IS state but its output power is outside of the specifications, complete the [“Clear the LOS-P Alarm” procedure on page 2-136](#).
- 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*.



Note Unplugging fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the procedures in the [“Alarm Procedures” section on page 2-21](#). For more detailed protection switching information, refer to the *Cisco ONS 15454 Procedure Guide*.

- 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 Card” procedure on page 2-219](#) 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 state.

- Step 13** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.224 OPWR-HFAIL

- Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Optical Power Fail High (OPWR-FAIL) alarm is raised by OPT-BST amplifier cards on the Line-3 TX port and OPT-PRE amplifier cards on the Line-1 TX port when an internal card problem on the card prevents the card from maintaining the output power setpoint at the output port and the card fails. It occurs on optical add/drop cards (AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, AD-4B-xx.x); demultiplexers (32 DMX-O); combiners (4MD-xx.x), and optical service channel cards (OSCM and OSC-CSM) when there is a failure on the VOA circuit.

Clear the OPWR-HFAIL Alarm

- Step 1** Complete the “[Clear the OPWR-HDEG Alarm](#)” procedure on page 2-158. (This procedure clears all optical power level degrade and fail alarms.)
- Step 2** 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.
-

2.7.225 OPWR-LDEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Low Degrade alarm occurs on all ports that use a setpoint, including the OPT-BST and OPT-PRE card AOTS ports in control power mode; the 32DMX, 32DMX-O, and 32MUX-O 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, and 32MUX-O 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 2-158. (This procedure clears all optical power level degrade and fail alarms.)
- Step 2** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.226 OPWR-LFAIL

- Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Failure alarm applies to 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, 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, 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 2-158. (This procedure clears all optical power degrade and fail alarms.)
- Step 2** 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.
-

2.7.227 OTUK-AIS

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Optical Transport Unit (OTUK) AIS condition (OTUK-AIS) 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 for the cards. OTUK-AIS is a secondary condition that indicates a more serious condition, such as the “[LOS \(OCN\)](#)” alarm on page 2-132, 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, or MXP_2.5G_10G cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the OTUK-AIS Condition

-
- Step 1** Complete the “[Clear the AIS Condition](#)” procedure on page 2-22.
- Step 2** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.228 OTUK-BDI

- 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, or 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 2-164.

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*.

Clear the OTUK-BDI Condition

-
- Step 1** Determine whether upstream nodes have the “OTUK-AIS” condition on page 2-161.
- 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.229 OTUK-LOF

- 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, or 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 or MXP card to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the OTUK-LOF Alarm

-
- Step 1** Complete the “Clear the LOF (OCN) Alarm” procedure on page 2-124.

- Step 2** 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.
-

2.7.230 OTUK-SD

- 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, or 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, or MXP_2.5G_10G cards to enable ITU-T G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Clear the OTUK-SD Condition

- Step 1** Complete the “[Clear the SD-L Condition](#)” procedure on page 2-180.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.231 OTUK-SF

- 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, or 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*.

Clear the OTUK-SF Condition

- Step 1** Complete the “[Clear the SD-L Condition](#)” procedure on page 2-180.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.232 OTUK-TIM

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The OTUK-TIM alarm 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 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 2-154.

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*.

Clear the OTUK-TIM Condition

-
- Step 1** Complete the “[Clear the TIM-P Alarm](#)” procedure on page 2-199.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.233 OUT-OF-SYNC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

The Ethernet Out of Synchronization (OUT-OF-SYNC) condition occurs on TXP-MR-2.5 and TXPP-MR-2.5 cards when the card ports are not correctly configured for the Ethernet payload data type.

Clear the OUT-OF-SYNC Condition

-
- Step 1** Double-click the alarmed card to display the card view.
- Step 2** Click the **Provisioning > Card** tabs.
- Step 3** In the **Payload Data Type** drop-down list, choose **Ethernet**.
- Step 4** Click **Apply**.
- Step 5** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.234 PDI-P

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: STSMON, STSTRM

The PDI Path condition (PDI-P) is a set of application-specific codes contained in the STS path overhead (POH) generated by the ONS node. 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, to the path selector in a downstream ONS node configured as part of a path protection. The PDI-P codes appear in the STS Signal Label (C2 byte).

The “AIS” condition on page 2-21 often accompanies the PDI-P condition. If the PDI-P is the only condition reported with the AIS, clear the PDI-P condition to clear the AIS condition. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid condition.

A PDI-P condition reported on the port of an OC-N card supporting a G1000-4 card circuit could result from the end-to-end Ethernet link integrity feature of the G1000-4. If the link integrity is the cause, it is typically accompanied by the “TPTFAIL (G1000)” alarm on page 2-200 or the “CARLOSS (G1000)” alarm on page 2-46 reported against one or both Ethernet ports terminating the circuit. If TPTFAIL or CARLOSS are reported against one or both of the Ethernet ports, troubleshooting the accompanying alarm clears the PDI-P condition.

A PDI-P condition reported on the port of an OC-N card 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 (G1000)” alarm on page 2-200 alarm reported against one or both packet over SONET (POS) ports terminating the circuit. If TPTFAIL is reported against one or both of packet over SONET (POS) ports, troubleshooting the accompanying alarm clears the PDI-P condition. Refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide* 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).



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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.



Caution

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

Clear the PDI-P Condition

-
- Step 1** Verify that all circuits terminating in the reporting card are in an active state:
- a. Click the **Circuits** tab.
 - b. Verify that the Status column lists the port as active.
 - c. If the Status column lists the port as incomplete, wait 10 minutes for the ONS 15454 to initialize fully. If the incomplete state does not change after full initialization, log onto <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 port is active, ensure that the signal source to the card reporting the alarm is working.

Step 3 If traffic is affected, complete the [“Delete a Circuit” procedure on page 2-217](#).



Caution Deleting a circuit could affect traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* 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 far-end 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 far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 8 If the condition does not clear, complete the [“Physically Replace a Card” procedure on page 2-219](#) for the optical/electrical (traffic) 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.



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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.235 PEER-NORESPONSE

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

The Peer Card Not Responding (PEER-NORESPONSE) alarm is raised by the switch agent 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 2-218](#) for the reporting card. For the LED behavior, see the [“Non-DWDM Card LED Activity During Reset” section on page 2-212](#).

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the [“Non-DWDM Card LED State After Successful Reset” section on page 2-213](#).

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

2.7.236 PLM-P

- Critical (CR), Service-Affecting (SA)
- Logical Objects: STSMON, STSTRM

A Payload Label Mismatch Path (PLM-P) alarm indicates that signal does not match its label. The condition occurs due to an invalid C2 byte value in the SONET path overhead.

For example, on non-DWDM nodes, this condition can 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).



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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.



Caution

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

Clear the PLM-P Alarm

- Step 1** Complete the [“Clear the PDI-P Condition” procedure on page 2-165](#).
- Step 2** 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.
-

2.7.237 PLM-V

- Major (MJ), Service-Affecting (SA)
- Logical Object: VT-TERM

A PLM VT Layer (PLM-V) alarm indicates that the content of the V5 byte in the SONET overhead is inconsistent or invalid. PLM-V occurs when ONS nodes interoperate with equipment that performs bit-synchronous mapping for DS-1. ONS nodes use 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 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.
-

2.7.238 PORT-CODE-MISM

- Critical (CR), Service-Affecting (SA)
- Logical Object: CLIENT

The Pluggable Port Security Code Mismatch (PORT-CODE-MISM) alarm refers to ML-Series Ethernet (traffic) cards, MXP_2.5G_10Gs, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5Gs. PORT-CODE-MISM occurs when the SFP connector that is plugged into the card is not supported by Cisco.

Clear the PORT-CODE-MISM Alarm

-
- Step 1** Unplug the SFP connector and fiber from the reporting card.
- Step 2** If the SFP connector has a latch securing the fiber cable, pull the latch upward to release the cable.
- Step 3** Pull the fiber cable straight out of the connector.
- Step 4** Plug the fiber into a Cisco-supported SFP connector.
- Step 5** If the new SFP connector has a latch, close the latch over the cable to secure it.
- Step 6** Plug the cabled SFP connector into the card port until it clicks.
- Step 7** 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.
-

2.7.239 PORT-COMM-FAIL

- Critical (CR), Service-Affecting (SA)
- Logical Object: CLIENT

The Port Communication Failure (PORT-COMM-FAIL) alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G card SFPs. It occurs when the card cannot communicate with the SFP.

Clear the PORT-COMM-FAIL Alarm

-
- Step 1** Replace the faulty SFP with a new SFP:
- Unplug the SFP connector and fiber from the ML-Series Ethernet (traffic) card.
 - If the SFP connector has a latch securing the fiber cable, pull the latch upward to release the cable.
 - Pull the fiber cable straight out of the connector.
 - Plug the fiber into a Cisco-supported SFP connector.
 - If the new SFP connector has a latch, close the latch over the cable to secure it.
 - Plug the cabled SFP connector into the ML-Series Ethernet card port until it clicks.
- Step 2** 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.
-

2.7.240 PORT-MISMATCH

- Critical (CR), Service-Affecting (CLIENT)
- Not Alarmed (NA), Non-Service Affecting (NSA) for FCMR
- Logical Objects: CLIENT, FCMR

The Pluggable Port Mismatch (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 IOS configuration. PORT-MISMATCH cannot be resolved in CTC. For information about provisioning the ML-Series Ethernet cards from the IOS interface, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide, Release 4.6*. If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).

2.7.241 PORT-MISSING

- Critical (CR), Service-Affecting (SA)
- Logical Object: CLIENT

The Pluggable Port Code Missing (PORT-MISSING) alarm applies to ML-Series Ethernet (traffic) card SFP connectors. The alarm indicates that the connector is not plugged into the card port.

For information about provisioning the ML-Series Ethernet cards from the IOS interface, refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide, Release 4.6*.

Clear the PORT-MISSING Alarm

-
- Step 1** If fiber is not plugged into the SFP connector, plug it in.

- Step 2** If the SFP connector has a latch, pull the latch over the connector.
 - Step 3** Push the SFP connector into the ML-Series Ethernet (traffic) card port until it clicks in place.
 - 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).
-

2.7.242 PRC-DUPID

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

The Procedural Error Duplicate Node ID (PRC-DUPID) 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 2-213](#).
 - 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 2-214](#) so that each node ID is unique.
 - Step 5** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).
-

2.7.243 PROTNA

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

The Protection Unit Not Available (PROTNA) alarm is caused by an OOS protection card when a TCC2 or XC10G cross-connect card that is 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 common control card (TCC2 or cross-connect), ensure that there is a redundant control 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):
 - a. In CTC, double-click the reporting card to display the card view (if the card is not an XC10G cross-connect card).

- b. Click the **Provisioning** tab.
 - c. Click the **State** of any in-service (IS) ports.
 - d. Choose **OOS** to take the ports out of service.
- Step 3** Complete the “[Reset a Traffic Card in CTC](#)” procedure on page 2-218 for the reporting card. For the LED behavior, see the “[Non-DWDM Card LED Activity During Reset](#)” section on page 2-212.
- Step 4** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the “[Non-DWDM Card LED State After Successful Reset](#)” section on page 2-213.
- Step 5** If the alarm does not clear, complete the “[Remove and Reinsert \(Reseat\) a Card](#)” procedure on page 2-219 for the reporting card.
- Step 6** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.244 PTIM

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Payload Type Identifier Mismatch (PTIM) 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, 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, 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.245 PWR-A

The PWR-A alarm is not used in this platform in this release. It is reserved for future development.

2.7.246 PWR-B

The PWR-A alarm is not used in this platform in this release. It is reserved for future development.

2.7.247 PWR-REDUN

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

The Redundant Power Capability Lost (PWR-REDUN) alarm applies to cards that have two built-in fuses (such as the TCC2 and newer optical [traffic] cards). The alarm indicates that one of the fuses has blown and must be serviced. When this alarm occurs, the card's power redundancy is lost because only one card power connection can contact one of the redundant power supplies.

Clear the PWR-REDUN Alarm

-
- Step 1** The card fuse is not field-replaceable. Complete the [“Physically Replace a Card” procedure on page 2-219](#).



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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.



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** Log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to arrange a card return for service.
-

2.7.248 RAI

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

The Remote Alarm Indication (RAI) condition signifies an end-to-end failure. The error condition is sent from one end of the SONET path to the other. RAI on the DS3XM-6 card indicates that the far-end node is receiving a DS-3 AIS.

Clear the RAI Condition

-
- Step 1** Complete the [“Clear the AIS Condition” procedure on page 2-22](#).
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.249 RCVR-MISS

- Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

A Facility Termination Equipment Receiver Missing (RCVR-MISS) 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 the DS-1 port or a possible mismatch of backplane equipment occurs, for example, an SMB connector or a BNC connector is connected 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.

**Caution**

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

Clear the RCVR-MISS Alarm

- Step 1** Ensure that the device attached to the DS-1 port is operational.
- 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 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.

2.7.250 RFI

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

The Remote Failure Indication (RFI) condition is similar to the “[RFI-L](#)” condition on page 2-174 but it is raised against an MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card when it has the “[AIS](#)” condition on page 2-21. The MXP or TXP cards will only raise AIS (or 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 2-217 and then recreate the circuit.

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

2.7.251 RFI-L

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

An RFI Line condition (RFI-L) 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-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 far-end node of the reporting ONS 15454.
- Step 2** Identify and clear any alarms, particularly the “[LOS \(OCN\)](#)” alarm on page 2-132.
- 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).
-

2.7.252 RFI-P

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

An RFI Path condition (RFI-P) 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-P condition in the reporting node. RFI-P occurs in the node that terminates a path.

Clear the RFI-P Condition

- Step 1** Verify that the ports are enabled and in service (IS) on the reporting ONS 15454:
- Confirm that the OC-N card shows a green LED in CTC or on the physical card.
A green LED indicates an active card. An amber 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 State column lists the port as IS.
 - If the State column lists the port as OOS, 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 2-204 or the “UNEQ-V” alarm on page 2-206.
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.253 RFI-V

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: VT-TERM

An RFI VT Layer (RFI-V) 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.



Caution

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

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*.
- Step 2** If connectors are correctly connected, verify that the DS-1 port is active and in service (IS):
- a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.
A green LED indicates an active card. An amber 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 State column lists the port as IS.
 - e. If the State column lists the port as OOS, 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 far-end of the reporting ONS 15454.
- Step 5** Clear alarms in the far-end node, especially the “UNEQ-P” alarm on page 2-204 or the “UNEQ-V” alarm on page 2-206.
- Step 6** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.254 RING-ID-MIS

- Major (MJ), Non-Service Affecting (NSA)
- Logical Objects: OCN, OSC-RING

The Ring ID Mismatch (RING-ID-MIS) 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.

Clear the RING-ID-MIS Alarm

-
- Step 1** Complete the [“Clear the RING-MISMATCH Alarm” procedure on page 2-176](#).
- Step 2** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.255 RING-MISMATCH

- Major (MJ), Service-Affecting (SA)
- Logical Objects: OCN, OSC-RING

A Procedural Error Mismatch Ring (RING-MISMATCH) alarm occurs when the ring name of the ONS 15454 that is reporting the alarm does not match the ring name of another ONS node in the BLSR. ONS nodes connected in a BLSR must have identical ring names to function. 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 number in the Ring Name field.
- Step 3** Log into the next ONS node in the BLSR.
- Step 4** Complete the [“Identify a BLSR Ring Name or Node ID Number” procedure on page 2-213](#).
- Step 5** If the ring name matches the ring name in the reporting ONS node, repeat [Step 4](#) for the next ONS node in the BLSR.
- Step 6** Complete the [“Change a BLSR Ring Name” procedure on page 2-213](#).
- Step 7** Verify that the ring map is correct.
- Step 8** 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.
-

2.7.256 RING-SW-EAST

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

The Ring Switch Is Active East Side (RING-SW-EAST) condition occurs when a ring switch occurs at the east side of two-fiber or four-fiber BLSR. The condition clears when the switch is cleared.

**Note**

RING-SW-EAST is an informational condition. It does not require troubleshooting.

2.7.257 RING-SW-WEST

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

The Ring Switch Is Active West Side (RING-SW-WEST) condition occurs when a ring switch occurs at the west side of a two-fiber or four-fiber BLSR. The condition clears when the switch is cleared.

**Note**

RING-SW-WEST is an informational condition. It does not require troubleshooting.

2.7.258 RSVP-HELLODOWN

- Minor (MN), Non-Service Affecting (NSA)
- Logical Object: UCP-NBR

The Resource Reservation Protocol (RSVP) Hello Down alarm (RSVP-HELLODOWN) occurs when the Hello protocol, which monitors UCP control channel status, is not available for reserving resources. The lack of availability can be caused by misconfiguration or loss of connectivity between the reporting node and its neighbor.

Clear the RSVP-HELLODOWN Alarm

-
- Step 1** Ensure that there are no physical layer problems between the reporting node and its neighbor.
- Step 2** Ensure that neighbor discovery (if enabled) has completed without any errors:
- a. In the node CTC view, click the **Provisioning > UCP > Neighbor** tabs.
 - b. Look for the neighbor ID and address. If it is present, neighbor discovery is working.
- Step 3** Ensure that RSVP hello is enabled on the neighbor node. If the neighbor is a Cisco ONS 15454, use the following procedure to ensure that RSVP Hello is enabled on the neighbor. If not, use the corresponding procedure on the core network element:
- a. In node view, click **View > Go to Network View**.
 - b. Double-click the neighbor node in the network map.
 - c. Click the **Provisioning > UCP > Node** tabs on this neighbor.

- d. Ensure that the RSVP area of the window contains entries in the Restart Time, Retransmit Interval, Recovery Time, and Refresh Interval fields.

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).

2.7.259 RUNCFG-SAVENEED

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

The Run Configuration Save Needed (RUNCFG-SAVENEED) condition occurs when you change the running configuration file for ML1000 and ML100T 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 CLI. If you do not save the change, the change is lost after the card reboots.

2.7.260 SD (CLIENT, TRUNK)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

An SD condition occurs when the quality of an optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card is so poor that the BER on the incoming optical line has passed the signal degrade threshold. The alarm applies to the card ports (DWDM client) 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 (CLIENT or TRUNK) Condition

Step 1 Complete the [“Clear the SD \(DS1, DS3\) Condition” procedure on page 2-179](#).

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

2.7.261 SD (DS1, DS3)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

A SD condition for DS-1 or DS-3 occurs when the quality of an electrical signal is so poor that the BER on the incoming optical line has passed the 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 on the ONS 15454 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 in-service (IS), out-of-service-auto-in-service (OOS-AINS), or auto-in-service (AINS) states, but not in out-of-service (OOS) state. The BER count increase associated with this alarm does not take an IS 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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.



Caution

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



Note

Some levels of BER errors (such as 10E_9) take a long period to raise or clear, about 9,000 seconds, or 150 minutes. If the SD threshold is provisioned at 10E_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 [“Verify BER Threshold Level” procedure on page 2-219](#).
- Step 2** 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 3** If the optical power level is okay, verify that optical receive levels are within the acceptable range.
- Step 4** 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*.
- Step 5** If the condition does not clear, verify that single-mode fiber is used.
- Step 6** If the fiber is the correct type, verify that a single-mode laser is used at the far-end node.

- Step 7** If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement.

**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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.

**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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.262 SD-L

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN

An SD Line condition (SD-L) is similar to the [“SD \(DS1, DS3\)” condition on page 2-178](#). It applies to the line level of the SONET signal.

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 [LOF \(EC1-12\)](#), [LOF \(OCN\)](#), [LOS \(EC1-12\)](#), or [LOS \(OCN\)](#).

Clear the SD-L Condition

- Step 1** Complete the [“Clear the SD \(DS1, DS3\) Condition” procedure on page 2-179](#).
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.263 SD-P

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

An SD Path condition (SD-P) is similar to the [“SD \(DS1, DS3\)” condition on page 2-178](#), but it applies to the path (STS) layer of the SONET overhead. A path or ST-level SD alarm travels on the B3 byte of the SONET overhead.

For path protected circuits, the BER threshold on the ONS 15454 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 2-179.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.264 SF (CLIENT, TRUNK)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

An SF for the DWDM client or trunk occurs when the quality of an optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card is so poor that the BER on the incoming optical line has passed the signal fail threshold. The alarm applies to the card ports (DWDM client) and the trunk carrying optical or electrical signals to the card.

Signal fail is defined by Telcordia as a soft 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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.



Caution

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

Clear the SF (CLIENT, TRUNK) Condition

-
- Step 1** Complete the “Clear the SD (DS1, DS3) Condition” procedure on page 2-179.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.265 SF (DS1, DS3)

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: DS1, DS3

An SF condition for the DS-1 or DS-3 signals occurs when the quality of the signal is so poor that the BER on the incoming optical line passed the 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 on the ONS 15454 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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.



Caution

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

Clear the SF (DS1, DS3) Condition

-
- Step 1** Complete the “[Clear the SD \(DS1, DS3\) Condition](#)” procedure on page 2-179.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.266 SF-L

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: EC1-12, OCN

An SF Line condition (SF-L) is similar to the “[SF \(DS1, DS3\)](#)” condition on page 2-182, 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 [LOF \(EC1-12\)](#), [LOF \(OCN\)](#), [LOS \(EC1-12\)](#), or [LOS \(OCN\)](#).

Clear the SF-L Condition

-
- Step 1** Complete the “[Clear the SD \(DS1, DS3\) Condition](#)” procedure on page 2-179.

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

2.7.267 SF-P

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

An SF Path condition (SF-P) is similar to an “[SF-L](#)” condition on page 2-182, 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 2-179.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.268 SFTWDOWN

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

A Software Download in Progress (SFTWDOWN) alarm occurs when the TCC2 is downloading or transferring software.

No action is necessary. Wait for the transfer or the software download to complete. If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).



Caution

It can take up to 30 minutes for software to be updated on a standby TCC2 card.



Note

SFTWDOWN is an informational alarm.

2.7.269 SH-INS-LOSS-VAR-DEG-HIGH

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

The Switch Insertion Loss Variation Degrade High (SH-INS-LOSS-VAR-DEG-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 will need to be replaced eventually.

2.7.269.1 Clear the SH-INS-LOSS-VAR-DEG-HIGH Alarm

-
- Step 1** For the alarmed card, complete the [“Physically Replace a Card” procedure on page 2-219](#) 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).
-

2.7.270 SH-INS-LOSS-VAR-DEG-LOW

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

The Switch Insertion Loss Variation Degrade Low (SH-INS-LOSS-VAR-DEG-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 will need to be replaced eventually.

2.7.270.1 Clear the SH-INS-LOSS-VAR-DEG-LOW Alarm

-
- Step 1** For the alarmed card, complete the [“Physically Replace a Card” procedure on page 2-219](#) 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).
-

2.7.271 SHUTTER-OPEN

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

The SHUTTER-OPEN alarm occurs if an OSC-CSM card laser shutter remains open after the [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 Alarm

-
- Step 1** Complete the [“Clear the LOS \(OTS\) Alarm” procedure on page 2-134](#).
- Step 2** If the SHUTTER-OPEN alarm still does not clear, it indicates that the unit shutter is not working properly. Complete the [“Physically Replace a Card” procedure on page 2-219](#).
-

- 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).
-

2.7.272 SNTP-HOST

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

The Simple Network Timing Protocol (Sntp) Host Failure alarm (Sntp-Host) indicates that an ONS node serving as an IP proxy for the other ONS nodes in the ring is not forwarding Sntp information to the other ONS nodes in the network. The forwarding failure can result from two causes: either the IP network attached to the ONS proxy node is experiencing problems, or the ONS 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.
- Step 3** If no network problems exist, ensure that the ONS 15454 proxy is provisioned correctly:
- a. In node view for the ONS node serving as the proxy, click the **Provisioning > General** tabs.
 - b. Ensure that the Use NTP/Sntp Server check box is checked.
 - c. If the Use NTP/Sntp Server check box is not checked, click it.
 - d. 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 *Cisco ONS 15454 Reference Manual* for more information on Sntp Host.
- Step 5** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.273 SPAN-SW-EAST

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

The Span Switch Is Active East Side (SPAN-SW-EAST) condition occurs when a span switch occurs at the east side of a four-fiber BLSR span. The condition clears when the switch is cleared.



Note

SPAN-SW-EAST is an informational condition. It does not require troubleshooting.

2.7.274 SPAN-SW-WEST

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

The Span Switch Is Active West Side (SPAN-SW-WEST) condition occurs when a span switch occurs at the west side of a four-fiber BLSR span. The condition clears when the switch is cleared.



Note

SPAN-SW-EAST is an informational condition. It does not require troubleshooting.

2.7.275 SQUELCH

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

The Ring Squelching Traffic (SQUELCH) 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 alarms appear on one or both of the nodes on either side of the isolated/failed node. The [“AIS-P” condition on page 2-22](#) also appears on all nodes in the ring except 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 at the lower-right outside edge of the shelf assembly.



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).



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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.

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.
- Step 3** If fiber continuity is okay, verify that the proper ports are in service:
- Confirm that the OC-N card shows a green LED in CTC or on the physical card.

A green LED indicates an active card. An amber 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 State column lists the port as IS.
- e. If the State column lists the port as OOS, 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 (traffic) card's receiver specifications. Refer to the *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 Card” procedure on page 2-219](#) 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.



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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.276 SQUELCHED

- Not Alarmed (NA), Non-Service Affecting (SA)
- Logical Object: CLIENT

The CLIENT Signal Squelched (SQUELCHED) alarm is raised by an MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G card when ITU-T G.709 monitoring is enabled and the card is operating in transparent mode. The alarm occurs on a far-end MXP or TXP card client port when the near end detects the [“LOF \(OCN\)” alarm on page 2-123](#) or the [“LOS \(OCN\)” alarm on page 2-132](#). The signal loss is indicated by the [“OTUK-AIS” alarm on page 2-161](#) in the OTN overhead. SQUELCHED can also indicate that the far-end trunk signal is invalid.

Clear the SQUELCHED Alarm

- Step 1** Verify that the far-end node and near-end node are not reporting the [“LOF \(OCN\)” alarm on page 2-123](#) or the [“LOS \(OCN\)” alarm on page 2-132](#). If so, complete the [“Clear the LOF \(OCN\) Alarm” procedure on page 2-124](#).

- Step 2** If no LOF or LOS is reported, verify that the far-end node and near-end are not reporting the trunk “WVL-MISMATCH” alarm on page 2-210 or the “DSP-FAIL” alarm on page 2-63. If either alarm is reported, complete the “Clear the WVL-MISMATCH alarm” procedure on page 2-210 or the “Clear the DSP-FAIL Alarm” procedure on page 2-64 as appropriate.
- Step 3** If no WVL-MISMATCH or DSP-FAIL is reported, verify that the near-end port reporting the SQUELCHED alarm is in service and is not in loopback:
- Double-click the client card to display the card view.
 - Click the **Maintenance > Loopback** tabs.
 - If the port State column says OOS or OOS_MT, click the cell to highlight it and choose **IS** from the pull-down menu. Changing the state to IS also clears any loopback provisioned on the port.
- Step 4** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.277 SQM

- Critical (CR), Service-Affecting (SA) for STSTRM
- Major (MJ), Service-Affecting (SA) for VT-TERM
- Logical Objects: STSTRM, VT-TERM

The Sequence Mismatch (SQM) alarm 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 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 2-217.
- Step 2** Recreate the circuit using the procedure in the *Cisco ONS 15454 Procedure Guide*.
- Step 3** 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.
-

2.7.278 SSM-DUS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, OCN, TRUNK

The Synchronization Status (SSM) Message Quality Changed to Do-Not-Use (DUS) condition (SSM-DUS) 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. It does not require troubleshooting.

2.7.279 SSM-FAIL

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, OCN, TRUNK

The SSM Failed alarm (SSM-FAIL) 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.280 SSM-LNC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

The SSM Local Node Clock (LNC) Traceable condition (SSM-LNC) 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. It does not require troubleshooting.

2.7.281 SSM-OFF

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, OCN, TRUNK

The SSM Off condition (SSM-OFF) applies to references used for timing the node. It occurs when the SSM for the reference has been turned off. The ONS 15454 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 2-189.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.282 SSM-PRC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

The SSM Primary Reference Clock (PRC) Traceable condition (SSM-PRC) occurs when the SONET transmission level is changed to PRC.



Note SSM-PRC is an informational condition. It does not require troubleshooting.

2.7.283 SSM-PRS

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Primary Reference Source (PRS) Traceable condition (SSM-PRS) occurs when the SSM transmission level is changed to Stratum 1 Traceable.



Note SSM-PRS is an informational condition. It does not require troubleshooting.

2.7.284 SSM-RES

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Reserved (RES) For Network Synchronization Use condition (SSM-RES) occurs when the synchronization message quality level is changed to RES.



Note SSM-RES is an informational condition. It does not require troubleshooting.

2.7.285 SSM-SDH-TN

The SSM-SDH-TN condition is not used in this platform in this release. It is reserved for future development.

2.7.286 SSM-SETS

The SSM-SETS condition is not used in this platform in this release. It is reserved for future development.

2.7.287 SSM-SMC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM SONET Minimum Clock (SMC) Traceable condition (SSM-SMC) 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. It does not require troubleshooting.

2.7.288 SSM-STU

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Synchronization Traceability Unknown (STU) condition (SSM-STU) 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** If the Sync Messaging **Enabled** check box for the BITS source is checked, uncheck the box.
- Step 3** If the Sync Messaging **Enabled** check box for the BITS source is not checked, check the box.
- Step 4** Click **Apply**.
- Step 5** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.289 SSM-ST2

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Stratum 2 (ST2) Traceable condition (SSM-ST2) occurs when the synchronization message quality level is changed to ST2.

**Note**

SSM-ST2 is an informational condition. It does not require troubleshooting.

2.7.290 SSM-ST3

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Stratum 3 (ST3) Traceable condition (SSM-ST3) occurs when the synchronization message quality level is changed to ST3.

**Note**

SSM-ST3 is an informational condition. It does not require troubleshooting.

2.7.291 SSM-ST3E

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Stratum 3E (ST3E) Traceable condition (SSM-ST3E) 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 not used for Generation 1.

**Note**

SSM-ST3E is an informational condition. It does not require troubleshooting.

2.7.292 SSM-ST4

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Stratum 4 (ST4) Traceable condition (SSM-ST4) 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. It does not require troubleshooting.

2.7.293 SSM-TNC

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, NE-SREF, OCN, TRUNK

The SSM Transit Node Clock (TNC) Traceable condition (SSM-TNC) occurs when the synchronization message quality level is changed to TNC.

**Note**

SSM-TNC is an informational condition. It does not require troubleshooting.

2.7.294 SWMTXMOD

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

The Switching Matrix Module Failure (SWMTXMOD) alarm occurs on the XC10G cross-connect card or a traffic card. 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 out of frame 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.

Clear the SWMTXMOD Alarm

-
- Step 1** If the card reporting the alarm is the standby XC10G cross-connect card, complete the [“Reset a Traffic Card in CTC” procedure on page 2-218](#) for the card. For the LED behavior, see the [“Non-DWDM Card LED Activity During Reset” section on page 2-212](#).
- Step 2** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the [“Non-DWDM Card LED State After Successful Reset” section on page 2-213](#).
- Step 3** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-219](#) 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 2-216](#).



Note After the active cross-connect goes into standby, 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 2-218](#) for the reporting card. For the LED behavior, see the [“Non-DWDM Card LED Activity During Reset” section on page 2-212](#).
- 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 [“Non-DWDM Card LED State After Successful Reset” section on page 2-213](#).
- Step 7** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-219](#) 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 2-216](#).
- Step 9** If the alarm does not clear after the cross-connect card side switch, complete the [“Reset a Traffic Card in CTC” procedure on page 2-218](#) for the reporting card. For the LED behavior, see the [“Non-DWDM Card LED Activity During Reset” section on page 2-212](#).
- Step 10** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the [“Non-DWDM Card LED State After Successful Reset” section on page 2-213](#).
- Step 11** If the alarm does not clear, complete the [“Remove and Reinsert \(Reseat\) a Card” procedure on page 2-219](#) for the traffic line card.

- Step 12** 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.
-

2.7.295 SWTOPRI

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

The Synchronization Switch to Primary Reference (SWTOPRI) 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. It does not require troubleshooting.

2.7.296 SWTOSEC

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

The Synchronization Switch to Secondary Reference (SYNCSEC) 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 2-195](#).
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.297 SWTOTHIRD

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

The Synchronization Switch to Third Reference (SWTOTHIRD) 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 2-195 or the “[SYNCSEC](#)” alarm on page 2-196.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.298 SYNC-FREQ

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: BITS, CLIENT, OCN, TRUNK

The Synchronization Reference Frequency Out Of Bounds (SYNC-FREQ) 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 Card](#)” procedure on page 2-219 for the TCC2 card.



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 active TCC2 to transfer the system software to the newly installed TCC2. Software transfer occurs in instances where different software versions exist on the two cards. During the transfer operation, the LEDs on the TCC2 flash fail and then the active/standby LED flashes. When the transfer completes, the TCC2 reboots and goes into standby mode after approximately three minutes.

- Step 3** If the SYNC-FREQ condition continues to report after replacing the TCC2 card, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.299 SYNCPRI

- Minor (MN), Non-Service Affecting (NSA)

- Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Primary Reference (SYNCPRI) 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 2-194.

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 reference is a BITS input, complete the “Clear the LOS (BITS) Alarm” procedure on page 2-127.
- 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 2-133.
- Step 5** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.300 SYNCSEC

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Secondary Reference (SYNCSEC) 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 2-194.

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 secondary reference is a BITS input, complete the “Clear the LOS (BITS) Alarm” procedure on page 2-127.
- 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 2-133.
- Step 6** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.301 SYNCTHIRD

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Third Reference (SYNCTHIRD) 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 card may have failed. The ONS 15454 often reports either the [“FRNGSYNC” condition on page 2-96](#) or the [“HLDOVRSYNC” condition on page 2-104](#) after a SYNCTHIRD 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 at the lower-right outside edge of the shelf assembly.

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 *Cisco ONS 15454 Procedure Guide*.
- Step 3** If the third timing source is a BITS input, complete the [“Clear the LOS \(BITS\) Alarm” procedure on page 2-127](#).
- 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 2-133](#).
- Step 5** If the third timing source uses the internal ONS 15454 timing, complete the [“Reset Active TCC2 Card and Activate Standby Card” procedure on page 2-217](#).
- 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” procedure on page 2-218](#). If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the [“Physically Replace a Card” procedure on page 2-219](#).
-

2.7.302 SYSBOOT

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

The System Reboot (SYSBOOT) alarm indicates that new software is booting on the TCC2 card. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes.

If it does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC to report a service-affecting problem (1 800 553-2447).

**Note**

SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

2.7.303 TIM

- Critical (CR), Service-Affecting (SA) for CLIENT, TRUNK
- Not Alarmed (NA), Non-Service Affecting (NSA) for OCN
- Logical Objects: CLIENT, OCN, TRUNK

The Section Trace Identifier Mismatch (TIM) alarm occurs when the expected J0 section trace string does not match the received section trace string.

If the condition 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 2-132](#) or the [“UNEQ-P” alarm on page 2-204](#). 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 or Condition

-
- 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 J1 Path Trace (port)** from the shortcut menu.
 - Step 5** Compare the Current Transmit String and the Current Expected String entries in the Edit J1 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.304 TIM-MON

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, TRUNK

The TIM Section Monitor Trace Identifier Mismatch (TIM-MON) alarm is similar to the [“TIM-P” alarm on page 2-199](#), but it applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or 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 2-199](#).
- Step 2** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.305 TIM-P

- Critical (CR), Service-Affecting (SA) for STSTRM
- Minor (MN), Non-Service Affecting (NSA) for STSMON
- Logical Objects: STSMON, STSTRM

The TIM Path alarm (TIM-P) is raised when the expected SONET path trace string does not match the received path trace string.

The alarm is raised on an incoming SONET span card in the following sequence:

- A signal error occurs on a DS-1 or DS-3 electrical signal;
- The electrical card reports the error to the TCC2;
- The TCC2 determines that the error is on the SONET overhead instead of the electrical signal itself, and raises the alarm against the receiving SONET port.

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, type 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 a new, incorrect value has been entered in the Current Transmit String field. This procedure applies to either situation.

TIM-P also occurs on a port that has previously been operating without alarms if DS-3 cables or optical fibers connecting the ports are switched or removed. TIM-P is usually accompanied by other alarms, such as the [“LOS \(OCN\)” alarm on page 2-132](#), the [“UNEQ-P” alarm on page 2-204](#), or the [“PLM-P” alarm on page 2-167](#). 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 or Condition” procedure on page 2-198](#).
- Step 2** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.7.306 TPTFAIL (FC_MR-4)

- Major (MJ), Service-Affecting (SA)
- Logical Object: FCMR

The Transport Fail (TPT-FAIL) alarm is raised against a local fibre channel (FC) port 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 also be raised against fibre channel cards if the remote FC card port is down from INC-SIG-LOSS or INC-SYNC-LOSS. 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).

Clear the TPTFAIL (FC_MR-4) 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.7.307 TPTFAIL (G1000)

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

The Transport (TPT) Layer Failure (TPTFAIL) alarm for the G-1000 Ethernet (traffic) cards indicates a break in the end-to-end Ethernet link integrity feature of the G1000-4 cards. TPTFAIL indicates a far-end 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 2-22, the “LOP-P” alarm on page 2-125, the “PDI-P” alarm on page 2-164, or the “UNEQ-P” alarm on page 2-204 exist on the SONET path used by the Ethernet port, the affected port causes a TPTFAIL alarm. Also, if the far-end G1000-4 Ethernet port is administratively disabled or it is reporting the “CARLOSS (G1000)” alarm on page 2-46, the C2 byte in the SONET path overhead indicates the “PDI-P” alarm on page 2-164, which in turn causes a TPTFAIL to be reported against the near-end port.

When a TPTFAIL alarm occurs, the near-end port is automatically disabled (transmit laser turned off). In turn, the laser shutoff can also cause the external Ethernet device attached at the near end 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.

Clear the TPTFAIL (G1000) Alarm

-
- Step 1** An occurrence of TPTFAIL on a G1000-4 port indicates either a problem with the SONET path that the port is using or with the far-end G1000-4 port that is mapped to the port. 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 2-164 is reported, the problem could be on the far-end G1000-4 port. Clear any alarms, such as CARLOSS, reported against the far-end port or card.
- Step 3** If the alarm does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.
-

2.7.308 TPTFAIL (ML100T, ML1000)

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

The TPT Layer Failure alarm for the ML100T or ML1000 Ethernet (traffic) cards indicates a break in the end-to-end POS link integrity feature of the ML-Series POS cards. TPTFAIL indicates a far-end 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 2-22, the “LOP-P” alarm on page 2-125, the “PDI-P” condition on page 2-164, or the “UNEQ-P” alarm on page 2-204 exist on the circuit used by the POS port, the affected port could report a TPTFAIL alarm. If the far-end ML-Series POS port is administratively disabled, it inserts an “AIS-P” condition on page 2-22 that is detected by the near-end port. The near-end port could report TPTFAIL in this event. If the POS port is misconfigured at the IOS CLI level, the misconfiguration causes the port to go down and report TPTFAIL.

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 *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide* for configuration information.
- Step 2** If the “PLM-P” alarm on page 2-167 is the only one reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Cisco ONS 15454 SONET/SDH ML-Series Multilayer Ethernet Card Software Feature and Configuration Guide* for configuration information.
- Step 3** If the “PDI-P” condition on page 2-164 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 2-46 is reported against the G-Series card, and if so, complete the “Clear the CARLOSS (G1000) Alarm” procedure on page 2-47.
- Step 4** If the “AIS-P” alarm on page 2-22, the “LOP-P” alarm on page 2-125, or the “UNEQ-P” alarm on page 2-204 is present, clear those alarms using the procedures in those sections.
- Step 5** 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.
-

2.7.309 TRMT

- Major (MJ), Service-Affecting (SA)

- Logical Object: DS1

A Missing Transmitter (TRMT) alarm occurs when there is a transmit failure on the 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 Card” procedure on page 2-219](#) 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.



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, call the Technical Assistance Center (TAC) at (1 800 553-2447) to discuss the failed card and possibly open an RMA.

2.7.310 TRMT-MISS

- Major (MJ), Service-Affecting (SA)
- Logical Object: DS1

A Facility Termination Equipment Transmitter Missing (TRMT-MISS) 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 connects 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 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.

2.7.311 TX-AIS

- Not Reported (NR), Non-Service Affecting (NSA)
- Logical Object: DS1

The (TX) Transmit Direction AIS condition (TX-AIS) is raised by the ONS backplane when it receives a far-end 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 2-132, 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 onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.312 TX-RAI

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: DS1

The Transmit Direction RAI condition (TX-RAI) 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 2-203.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.313 UNC-WORD

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: TRUNK

The Uncorrected FEC Word (UNC-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 dB reduction in Signal to Noise Ratio (SNR).

Clear the UNC-WORD Condition

-
- Step 1** Complete the “[Clear the SD-L Condition](#)” procedure on page 2-180.

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

2.7.314 UNEQ-P

- Critical (CR), Service-Affecting (SA)
- Logical Objects: STSMON, STSTRM

A signal label mismatch fault (SLMF) UNEQ Path alarm (UNEQ-P) 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 an incomplete circuit or an empty VT tunnel. UNEQ-P occurs in the node that terminates a path.



Note

If you have created a new circuit but it has no signal, a UNEQ-P alarm is reported on the OC-N cards and the “AIS-P” condition on page 2-22 is reported on the terminating cards. These alarms clear when the circuit carries a signal.



Caution

Deleting a circuit affects traffic.



Caution

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

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 2-217](#).
- If an error message dialog box appears, the VT tunnel is valid and not the cause of the alarm.
- If any other columns contain VTT, repeat [Figure 2-1 Step 6](#).

- Step 7** If all ONS nodes in the ring appear in the CTC network view, determine whether the circuits are complete:
- Click the **Circuits** tab.
 - Verify that INCOMPLETE is not listed in the Status column of any circuits.
- Step 8** If you find circuits listed as incomplete, 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 incomplete circuits are not needed or are not passing traffic, delete the incomplete circuits. Complete the [“Delete a Circuit” procedure on page 2-217](#).
- Step 10** Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide*.
- 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 far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15454 Procedure Guide*.

**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).

**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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.

- Step 13** If the alarm does not clear, complete the [“Physically Replace a Card” procedure on page 2-219](#) 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.

**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 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.
-

2.7.315 UNEQ-V

- 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-P. 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).



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. Use of controls or adjustments or performance of procedures other than those specified could result in hazardous radiation exposure.



Caution

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

Clear the UNEQ-V Alarm

-
- Step 1** Complete the “[Clear the UNEQ-P Alarm](#)” procedure on page 2-204.
- Step 2** 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.
-

2.7.316 VCG-DEG

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: VCG

The VCAT Group Degraded (VCG-DEG) 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 2-157. 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 \(CLIENT\)](#), page 2-127 or [LOS \(OTS\)](#), page 2-134.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.317 VCG-DOWN

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Object: VCG

The VCAT Group Down (VCG-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 \(CLIENT\)” alarm on page 2-127](#).

Clear the VCG-DOWN Condition

-
- Step 1** Complete the [“Clear the VCG-DEG Condition” procedure on page 2-207](#).
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.318 VOA-HDEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The variable optical attenuator (VOA) Degrade High alarm (VOA-HDEG) applies to amplifiers (OPT-BST and OPT-PRE), band add/drop cards (AD-1B-xx.x and AD-4B-xx), and to channel add/drop cards (AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x) on the Line-1 TX port. It occurs when internal problem in the card keeps the VOA attenuation from maintaining the setpoint.

Clear the VOA-HDEG Alarm

-
- Step 1** This alarm does not immediately affect traffic, but to clear the alarm, you will eventually need to complete the [“Physically Replace a Card” procedure on page 2-219](#).

**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. Refer to the *Cisco ONS 15454 SDH Procedure Guide* for information.



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 condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.319 VOA-HFAIL

- Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA Fail High alarm (VOA-HFAIL) occurs on OPT-BST and OPT-PRE amplifier cards when the amplifier VOA component is broken.

Clear the VOA-HFAIL Alarm

Step 1 Complete the [“Physically Replace a Card” procedure on page 2-219](#) 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. Refer to the *Cisco ONS 15454 SDH Procedure Guide* for information.



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 condition 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.

2.7.320 VOA-LDEG

- Minor (MN), Non-Service Affecting (NSA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA Degrade Low alarm (VOA-LDEG) applies to amplifiers (OPT-BST and OPT-PRE), band add/drop cards (AD-1B-xx.x and AD-4B-xx), and to channel add/drop cards (AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x) on the Line-1 TX port. It occurs when internal problem in the card keeps the VOA attenuation from reaching the setpoint.

Clear the VOA-LDEG Alarm

Step 1 This alarm does not immediately affect traffic, but to clear the alarm, you will eventually need to complete the “[Physically Replace a Card](#)” procedure on page 2-219 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. Refer to the *Cisco ONS 15454 SDH Procedure Guide* for information.

**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 condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

2.7.321 VOA-LFAIL

- Critical (CR), Service-Affecting (SA)
- Logical Objects: AOTS, OCH, OMS, OTS

The VOA Fail Low alarm (VOA-LFAIL) occurs on OPT-BST and OPT-PRE amplifier cards when the amplifier VOA component is broken.

Clear the VOA-LFAIL Alarm

Step 1 Complete the “[Physically Replace a Card](#)” procedure on page 2-219 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. Refer to the *Cisco ONS 15454 SDH Procedure Guide* for information.

**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 condition 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.

2.7.322 WKSWPR

- Not Alarmed (NA), Non-Service Affecting (NSA)

- Logical Objects: CLIENT, EQPT, OCN, STSMON, TRUNK, VT-MON

The Working Switched To Protection (WKSWPR) condition occurs when a line experiences the “LOS (OCN)” alarm on page 2-132, the “SF (DS1, DS3)” condition on page 2-182, or the “SD (CLIENT, TRUNK)” condition on page 2-178.

Clear the WKSWPR Condition

-
- Step 1** Complete the “Clear the LOS (OCN) Alarm” procedure on page 2-133.
- Step 2** If the condition does not clear, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).
-

2.7.323 WTR

- Not Alarmed (NA), Non-Service Affecting (NSA)
- Logical Objects: CLIENT, EQPT, OCN, STSMON, TRUNK, VT-MON

The Wait To Restore (WTR) condition occurs when the “WKSWPR” condition on page 2-209 is raised 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. It does not require troubleshooting.

2.7.324 WVL-MISMATCH

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

The Equipment Wavelength Mismatch (WVL-MISMATCH) alarm applies to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or 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, 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, 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 pull-down menu and choose the correct wavelength.
- Step 8** Click **Apply**.
- Step 9** 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 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 as the standard DS-3 card.

Table 2-9 DS3-12E Line Alarms

Alarm	UNFRAMED	M13	CBIT
LOS	Yes	Yes	Yes
AIS	Yes	Yes	Yes
LOF	No	Yes	Yes
IDLE	No	Yes	Yes
RAI	No	Yes	Yes
Terminal Lpbk	Yes	Yes	Yes
Facility Lpbk	Yes	Yes	Yes
FE Lpbk	No	No	Yes
FE Common Equipment Failure	No	No	Yes
FE Equipment Failure-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	No	No	Yes

2.9 DWDM and Non-DWDM Card LED Activity

DWDM cards and non-DWDM cards in the ONS 15454 system have somewhat different LED activity. The following sections list the LED behavior that occurs during card insertion, resetting, or in the case of the non-DWDM system, XC10G cross-connect card side-switching.

2.9.1 DWDM Card LED Activity After Insertion

When a 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 far-end counterparts and a signal is present.

2.9.2 Non-DWDM 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 far-end counterparts and a signal is present.

2.9.3 DWDM Card LED Activity During Reset

When a 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.

2.9.4 Non-DWDM 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.

2.9.5 Non-DWDM 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.

2.9.6 Non-DWDM 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 Common Procedures in Alarm Troubleshooting

This section gives common procedures that are frequently used when troubleshooting alarms. For more information about ring or node traffic switching operations, refer to the *Cisco ONS 15454 Procedure Guide*.

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.

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.

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** Enter the new ID in the field.
 - Step 8** Click **Apply**.
-

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** Verify that each node in the ring appears on the ring map with a node ID and IP address.
 - Step 6** Click **Close**.
-

Verify or Create Node DCC Terminations



Note Portions of this procedure are different for DWDM.

- 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 > DCC/GCC/OSC** tabs.
- 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:
 - a. Click **Create**.

- b. 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.
 - c. In the Port State area, click the **Set to IS** radio button.
 - d. Verify that the Disable OSPF on Link check box is unchecked.
 - e. Click **OK**.
-

Lock Out a BLSR Span

- 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 **Maintenance > BLSR** tabs.
 - Step 3** Click the BLSR row table cell under the West Switch column to reveal the pull-down menu.
 - Step 4** Choose **Lockout Protect Span** and click **Apply**.
 - Step 5** Click **OK** on the BLSR Operations 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** In node view, click the **Maintenance > BLSR** tabs.
 - Step 3** Click the BLSR row table cell under the West Switch column to reveal the pull-down menu.
 - Step 4** Choose **CLEAR** and click **Apply**.
 - Step 5** Click **OK** on the BLSR Operations dialog box.
-

Clear a Path Protection Lockout

- 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 **View > Go to Network View**.
 - Step 3** Right-click the span where you want to clear the switch. Choose **Circuits** from the shortcut menu.
 - Step 4** In the Circuits on Span dialog box, choose **CLEAR** from the Perform UPSR Span Switching pull-down menu to remove a previously set switch command. Click **Apply**.
 - Step 5** In the Confirm UPSR Switch dialog box, click **Yes**.
 - Step 6** In the Protection Switch Result dialog box, click **OK**.
- In the Circuits on Span window, the switch state for all path protection circuits is CLEAR.
-

Switch Protection Group Traffic with an External Switching Command

-
- Step 1** Log into a node on the network. If you are already logged in, continue with [Step 2](#).
 - Step 2** Display node view.
 - Step 3** Click the **Maintenance > Protection** tabs.
 - Step 4** Click the protection group that contains the reporting card.
 - Step 5** Click the Working or active card of the selected group.
 - Step 6** Click **Manual** and **Yes** in the confirmation dialog box.
-

Side Switch the Active and Standby XC10G Cross-Connect cards



Caution The cross-connect card side switch is traffic-affecting.

-
- Step 1** Log into a node on the network. 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 “[Non-DWDM Cross-Connect LED Activity During Side Switch](#)” section on page 2-213 for LED information.
-

Clear a Protection Group External Switching Command

-
- 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 **Maintenance > Protection** tabs.
 - Step 3** Double-click the protection group that contains the reporting card.
 - Step 4** Highlight either selected group.
 - Step 5** Click **Clear** and click **Yes** in the confirmation dialog box.
-

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.
-

Clear a G-Series, OCN, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G Loopback

-
- 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** tab.
 - 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 pull-down menu and select None.
 - Step 6** In the 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 pull-down menu and select **IS**.
 - Step 8** Click **Apply**.
-

Reset Active TCC2 Card and Activate Standby Card



Caution The TCC2 card reset can be traffic-affecting.

- 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 card.

If you are looking at the physical ONS 15454, the ACT/SBY LED of the active TCC2 is green. The ACT/STBLY LED of the standby TCC2 is amber.



Caution Resetting an active TCC2 can cause data or provisioning loss if certain alarms—such as BKUPMEMP, CONTBUS-A-18, CONTBUS-B-18, CONTBUS-IO-A, CONTBUS-IO-B, DBOSYNC, DUP-IPADDR, DUP-NODENAME, HITEMP, I-HITEMP, MEM-GONE, PROTNA, SFTWDOWN, or SYSBOOT—are present and unresolved. Use the reset process only after resolving any of the named alarms. (You can use the procedure in the process of resolving the named alarms if instructed to do so.) If there is any doubt about whether the reset can cause data loss, log onto <http://www.cisco.com/techsupport> for more information or call Cisco TAC (1 800 553-2447).

- Step 3** Right-click the active TCC2 card in CTC.
- Step 4** Choose **Reset Card** from the shortcut menu.

Step 5 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.

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 “[Non-DWDM Card LED State After Successful Reset](#)” section on page 2-213.

Double-click the node and ensure that the reset TCC2 card is in standby mode and that the other TCC2 card is active.

- If you are looking at the physical ONS 15454, the ACT/SBY LED of the active TCC2 is green. The ACT/STBLY LED of the standby TCC2 is amber.
- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15454, the active TCC2 ACT/SBY LED is green, and the LED of the standby TCC2 is amber.

Remove and Reinsert (Reseat) the Standby TCC2



Caution

Do not perform this action without the supervision and direction of Cisco TAC (1 800 553-2447).



Caution

The TCC2 card reseat can be traffic-affecting.



Note

Before you reset the TCC2, 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 Ensure that the TCC2 you want to reset is in standby mode. On the TCC2 card, the ACT/SBY (Active/Standby) LED is amber when the TCC2 is in standby mode.

Step 3 When the TCC2 is in standby mode, unlatch both the top and bottom ejectors on the TCC2 card.

Step 4 Physically pull the card at least partly out of the slot until the lighted LEDs turn off.

Step 5 Wait 30 seconds. Reinsert the card and close the ejectors.



Note

The TCC2 will take several minutes to reboot and will display the amber standby LED after rebooting. Refer to the *Cisco ONS 15454 Procedure Guide* for more information about LED behavior during TCC2 card reboots.

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 Slots 1 to 4 and 14 to 17 or Slots 5, 6, 12, and 13 reporting the alarm.
 - Step 3** Right-click and choose **RESET CARD** from the shortcut menu.
 - Step 4** Click **Yes** in the Resetting Card dialog box.
-

Verify 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**.
-

Physically Replace a 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 [“Switch Protection Group Traffic with an External Switching Command” procedure on page 2-216](#) for more information.

- 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.
-

Remove and Reinsert (Reseat) a 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.

Remove and Reinsert 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.
