C H A P T E R **2**

Alarm Troubleshooting

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

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco ONS 15454 alarm and condition. Table 2-1 on page 2-2 through Table 2-4 on page 2-3 give lists of ONS 15454 alarms organized by severity. Table 2-5 on page 2-5 gives a list of alarm organized alphabetically. Table 2-6 on page 2-7 gives 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*.

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/tac for more information or call the Cisco Technical Assistance Center (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 alarm index by severity tables group alarms and conditions by the severity displayed in the CTC Alarms window in the severity (SEV) column. The default standby severity for all ONS 15454 alarms on unprovisioned card ports is Minor, Non-Service Affecting, as defined in Telcordia GR-474. All severities listed in the alarm entry are the default for the active card, if applicable. Alarm severities can be altered from default settings for individual alarms or groups of alarms on a card, node, or network basis.

> ✎
> **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 2-30	IMPROPRMVL, page 2-87	MEA (BP), page 2-114
BKUPMEMP, page 2-36	LOF (DS-3), page 2-95	MEA (EQPT), page 2-115
CKTDOWN, page 2-43	LOF (EC-N), page 2-96	MEA (FAN), page 2-117
COMIOXC, page 2-46	LOF (OC-N), page 2-96	MFGMEM, page 2-118
CTNEQPT-PBPROT, page 2-50	LOM, page 2-98	OTUK-LOF, page 2-124
CTNEQPT-PBWORK, page 2-52	LOP-P, page 2-98	PLM-P, page 2-128
EQPT, page 2-59	LOS (DS-3), page 2-102	SWMTXMOD, page 2-150
EQPT-MISS, page 2-60	LOS (EC-N), page 2-103	TIM-P, page 2-155
FAN, page 2-70	LOS (OC-N), page 2-105	UNEQ-P, page 2-159
HITEMP, page 2-86	MEA (AIP), page 2-114	

2.1.2 Major Alarms (MJ)

Table 2-2 lists Major alarms.

Table 2-2   Major Alarm Index

APSCM, page 2-25	E-W-MISMATCH, page 2-61	PORT-COMM-FAIL, page 2-131
APSCNMIS, page 2-26	EXTRA-TRAF-PREEMPT, page 2-65	PORT-MISMATCH, page 2-131
BLSROSYNC, page 2-36	FANDEGRADE, page 2-71	PORT-MISSING, page 2-131
CARLOSS (EQPT), page 2-37	GCC-EOC, page 2-83	PRC-DUPID, page 2-132
CARLOSS (E-Series), page 2-38	INVMACADR, page 2-90	RCVR-MISS, page 2-135
CARLOSS (G-Series), page 2-39	LOF (BITS), page 2-93	RING-MISMATCH, page 2-138
CARLOSS (ML-Series), page 2-42	LOF (DS-1), page 2-94	SQUELCHED, page 2-146
CONTBUS-A-18, page 2-47	LOP-V, page 2-99	SYSBOOT, page 2-155
CONTBUS-B-18, page 2-47	LOS (BITS), page 2-101	TPTFAIL (G-Series), page 2-156
CONTBUS-IO-A, page 2-48	LOS (DS-1), page 2-101	TPTFAIL (ML-Series), page 2-157
CONTBUS-IO-B, page 2-49	MEM-GONE, page 2-117	TRMT, page 2-158
DBOSYNC, page 2-54	OTUK-IAE, page 2-124	TRMT-MISS, page 2-158
DSP-COMM-FAIL, page 2-55	PEER-NORESPONSE, page 2-128	UNEQ-V, page 2-161
DSP-FAIL, page 2-55	PORT-CODE-MISM, page 2-130	WVL-MISMATCH, page 2-162
EOC, page 2-57		

2.1.3 Minor Alarms (MN)

Table 2-3 lists Minor alarms.

Table 2-3   Minor Alarm Index

2.1.4 Conditions (NA or NR)

Table 2-4 lists Not Alarmed or Not Reported conditions.

Table 2-4   Conditions Index

Table 2-4   Conditions Index (continued)

BAT-A-HGH-VLT, page 2-34	KB-PASSTHR, page 2-90	SD, page 2-139
BAT-A-LOW-VLT, page 2-35	LAN-POL-REV, page 2-90	SD-L, page 2-140
BAT-B-HGH-VLT, page 2-35	LKOUTPR-S, page 2-91	SD-P, page 2-141
BAT-B-LOW-VLT, page 2-35	LOCKOUT-REQ, page 2-93	SF, page 2-141
CLDRESTART, page 2-45	LOCKOUT-REQ-RING, page 2-93	SF-L, page 2-142
DS3-MISM, page 2-54	LPBKCRS, page 2-107	SF-P, page 2-142
EXERCISE-RING-REQ, page 2-64	LPBKDS1FEAC, page 2-107	SPAN-SW-EAST, page 2-144
EXERCISE-SPAN-REQ, page 2-64	LPBKDS1FEAC-CMD, page 2-108	SPAN-SW-WEST, page 2-144
FAILTOSW, page 2-65	LPBKDS3FEAC, page 2-108	SQUELCH, page 2-145
FAILTOSW-PATH, page 2-66	LPBKDS3FEAC-CMD, page 2-108	SSM-DUS, page 2-147
FAILTOSWR, page 2-67	LPBKFACILITY (DS-1 or DS-3), page 2-109	SSM-LNC, page 2-147
FAILTOSWS, page 2-68	LPBKFACILITY (EC-N), page 2-109	SSM-OFF, page 2-147
FE-AIS, page 2-71	LPBKFACILITY (OC-N), page 2-110	SSM-PRC, page 2-148
FE-DS1-MULTLOS, page 2-71	LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110	SSM-PRS, page 2-148
FE-DS1-NSA, page 2-72	LPBKTERMINAL (G-Series), page 2-111	SSM-RES, page 2-148
FE-DS3-SA, page 2-74	MAN-REQ, page 2-112	SSM-SMC, page 2-148
FE-DS1-SNGLLOS, page 2-73	MANRESET, page 2-112	SSM-ST2, page 2-149
FE-DS3-NSA, page 2-73	MANSWTOINT, page 2-112	SSM-ST3, page 2-149
FE-DS3-SA, page 2-74	MANSWTOPRI, page 2-112	SSM-ST3E, page 2-149
FE-EQPT-NSA, page 2-74	MANSWTOSEC, page 2-113	SSM-ST4, page 2-149
FE-EXERCISING-RING, page 2-75	MANSWTOTHIRD, page 2-113	SSM-STU, page 2-150
FE-EXERCISING-SPAN, page 2-75	MANUAL-REQ-RING, page 2-113	SSM-TNC, page 2-150
FE-FRCDWKSWPR-RING, page 2-75	MANUAL-REQ-SPAN, page 2-113	SWTOPRI, page 2-152
FE-FRCDWKSWPR-SPAN, page 2-76	NO-CONFIG, page 2-118	SWTOSEC, page 2-152
FE-IDLE, page 2-76	ODUK-AIS-PM, page 2-119	SWTOTHIRD, page 2-152
FE-LOCKOUTOFPR-SPAN, page 2-77	ODUK-BDI-PM, page 2-120	SYNC-FREQ, page 2-153
FE-LOF, page 2-77	ODUK-LCK-PM, page 2-120	UNC-WORD, page 2-159
FE-LOS, page 2-78	ODUK-OCI-PM, page 2-121	WKSWPR, page 2-162
FE-MANWKSWPR-RING, page 2-78	ODUK-SD-PM, page 2-121	WTR, page 2-162

2.2 Alarms and Conditions Indexed By Alphabetical Entry

Table 2-5 lists alarms and conditions by the name displayed on the CTC Alarms window or Conditions window.

Table 2-5   Alphabetical Alarm Index

AIS, page 2-21	FE-LOF, page 2-77	ODUK-BDI-PM, page 2-120
AIS-L, page 2-22	FE-LOS, page 2-78	ODUK-LCK-PM, page 2-120
AIS-P, page 2-22	FE-MANWKSWPR-RING, page 2-78	ODUK-OCI-PM, page 2-121
AIS-V, page 2-22	FE-MANWKSWPR-SPAN, page 2-79	ODUK-SD-PM, page 2-121
APSB, page 2-23	FEPRLF, page 2-79	ODUK-SF-PM, page 2-122
APSCDFLTK, page 2-24	FORCED-REQ, page 2-80	ODUK-TIM-PM, page 2-122
APSC-IMP, page 2-24	FORCED-REQ-RING, page 2-80	OTUK-AIS, page 2-123
APSCINCON, page 2-25	FORCED-REQ-SPAN, page 2-81	OTUK-BDI, page 2-123
APSCM, page 2-25	FRCDSWTOINT, page 2-81	OTUK-IAE, page 2-124
APSCNMIS, page 2-26	FRCDSWTOPRI, page 2-81	OTUK-LOF, page 2-124
APSMM, page 2-27	FRCDSWTOSEC, page 2-81	OTUK-SD, page 2-125
AS-CMD, page 2-28	FRCDSWTOTHIRD, page 2-82	OTUK-SF, page 2-125
AS-MT, page 2-29	FRNGSYNC, page 2-82	OTUK-TIM, page 2-125
AUD-LOG-LOSS, page 2-29	FSTSYNC, page 2-82	PDI-P, page 2-126
AUD-LOG-LOW, page 2-30	FULLPASSTHR-BI, page 2-82	PEER-NORESPONSE, page 2-128
AUTOLSROFF, page 2-30	GCC-EOC, page 2-83	PLM-P, page 2-128
AUTORESET, page 2-31	HI-LASERBIAS, page 2-83	PLM-V, page 2-130
AUTOSW-AIS, page 2-31	HI-LASERTEMP, page 2-84	PORT-CODE-MISM, page 2-130
AUTOSW-LOP (STSMON), page 2-32	HI-RXPOWER, page 2-84	PORT-MISSING, page 2-131
AUTOSW-LOP (VTMON), page 2-32	HI-RXTEMP, page 2-85	PORT-COMM-FAIL, page 2-131
AUTOSW-PDI, page 2-32	HITEMP, page 2-86	PORT-MISMATCH, page 2-131
AUTOSW-SDBER, page 2-33	HI-TXPOWER, page 2-86	PRC-DUPID, page 2-132
AUTOSW-SFBER, page 2-33	HLDOVRSYNC, page 2-87	PROTNA, page 2-132
AUTOSW-UNEQ (STSMON), page 2-34	IMPROPRMVL, page 2-87	PWR-A, page 2-133
AUTOSW-UNEQ (VTMON), page 2-34	INC-ISD, page 2-89	PWR-B, page 2-134
BAT-A-HGH-VLT, page 2-34	INHSWPR, page 2-89	PWR-REDUN, page 2-134
BAT-A-LOW-VLT, page 2-35	INHSWWKG, page 2-90	RAI, page 2-135
BAT-B-HGH-VLT, page 2-35	INVMACADR, page 2-90	RCVR-MISS, page 2-135
BAT-B-LOW-VLT, page 2-35	KB-PASSTHR, page 2-90	RFI-L, page 2-136
BKUPMEMP, page 2-36	LAN-POL-REV, page 2-90	RFI-P, page 2-136
BLSROSYNC, page 2-36	LASEREOL, page 2-91	RFI-V, page 2-137
CARLOSS (EQPT), page 2-37	LKOUTPR-S, page 2-91	RING-MISMATCH, page 2-138
CARLOSS (E-Series), page 2-38	LMP-HELLODOWN, page 2-92	RING-SW-EAST, page 2-138
CARLOSS (G-Series), page 2-39	LMP-NDFAIL, page 2-92	RING-SW-WEST, page 2-138
CARLOSS (ML-Series), page 2-42	LOCKOUT-REQ, page 2-93	RSVP-HELLODOWN, page 2-138
CKTDOWN, page 2-43	LOCKOUT-REQ-RING, page 2-93	RUNCFG-SAVENEED, page 2-139

Table 2-5   Alphabetical Alarm Index (continued)

Table 2-5   Alphabetical Alarm Index (continued)

FE-DS1-NSA, page 2-72	MANUAL-REQ-SPAN, page 2-113	TIM-P, page 2-155
FE-DS1-SA, page 2-72	MEA (AIP), page 2-114	TPTFAIL (G-Series), page 2-156
FE-DS1-SNGLLOS, page 2-73	MEA (BP), page 2-114	TPTFAIL (ML-Series), page 2-157
FE-DS3-NSA, page 2-73	MEA (EQPT), page 2-115	TRMT, page 2-158
FE-DS3-NSA, page 2-73	MEA (FAN), page 2-117	TRMT-MISS, page 2-158
FE-EQPT-NSA, page 2-74	MEM-GONE, page 2-117	UNC-WORD, page 2-159
FE-EXERCISING-RING, page 2-75	MEM-LOW, page 2-118	UNEQ-P, page 2-159
FE-EXERCISING-SPAN, page 2-75	MFGMEM, page 2-118	UNEQ-V, page 2-161
FE-FRCDWKSWPR-RING, page 2-75	NO-CONFIG, page 2-118	WKSWPR, page 2-162
FE-FRCDWKSWPR-SPAN, page 2-76	NOT-AUTHENTICATED, page 2-119	WTR, page 2-162
FE-IDLE, page 2-76	ODUK-AIS-PM, page 2-119	WVL-MISMATCH, page 2-162
FE-LOCKOUTOFPR-SPAN, page 2-77		

2.3 Alarm Index by Alarm Type

Table 2-6 gives the name and page number of every alarm in the chapter organized by alarm type.

Table 2-6   Alarm Index by Alarm Type

AEP: EQPT, page 2-59
AEP: MFGMEM, page 2-118
AIP: INVMACADR, page 2-90
AIP: MEA (AIP), page 2-114
AIP: MFGMEM, page 2-118
BITS: LOS (BITS), page 2-101
BITS: AIS, page 2-21
BITS: LOF (BITS), page 2-93
BITS: SSM-DUS, page 2-147
BITS: SSM-FAIL, page 2-147
BITS: SSM-OFF, page 2-147
BITS: SSM-PRS, page 2-148
BITS: SSM-RES, page 2-148
BITS: SSM-SMC, page 2-148
BITS: SSM-ST2, page 2-149
BITS: SSM-ST3, page 2-149
BITS: SSM-ST3E, page 2-149
BITS: SSM-ST4, page 2-149
BITS: SSM-STU, page 2-150

Table 2-6   Alarm Index by Alarm Type (continued)

BITS: SSM-TNC, page 2-150
BP: AS-CMD, page 2-28
BP: MEA (BP), page 2-114
BP: MFGMEM, page 2-118
CC: LMP-HELLODOWN, page 2-92
CC: LMP-NDFAIL, page 2-92
CKT: CKTDOWN, page 2-43
DS1: AIS, page 2-21
DS1: AS-CMD, page 2-28
DS1: AS-MT, page 2-29
DS1: LOF (DS-1), page 2-94
DS1: LOS (DS-1), page 2-101
DS1: LPBKDS1FEAC, page 2-107
DS1: LPBKDS1FEAC-CMD, page 2-108
DS1: LPBKFACILITY (DS-1 or DS-3), page 2-109
DS1: LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110
DS1: RAI, page 2-135
DS1: RCVR-MISS, page 2-135
DS3: SD, page 2-139
DS3: SF, page 2-141
DS1: TRMT, page 2-158
DS1: TRMT-MISS, page 2-158
DS3: AIS, page 2-21
DS3: AS-CMD, page 2-28
DS3: AS-MT, page 2-29
DS3: DS3-MISM, page 2-54
DS3: FE-AIS, page 2-71
DS3: FE-DS1-MULTLOS, page 2-71
DS3: FE-DS1-NSA, page 2-72
DS3: FE-DS1-SA, page 2-72
DS3: FE-DS1-SNGLLOS, page 2-73
DS3: FE-DS3-NSA, page 2-73
DS3: FE-DS3-SA, page 2-74
DS3: FE-EQPT-NSA, page 2-74
DS3: FE-IDLE, page 2-76
DS3: FE-LOF, page 2-77
DS3: FE-LOS, page 2-78

Table 2-6   Alarm Index by Alarm Type (continued)

DS3: INC-ISD, page 2-89
DS3: LOF (DS-3), page 2-95
DS3: LOS (DS-3), page 2-102
DS3: LPBKDS1FEAC, page 2-107
DS3: LPBKDS3FEAC, page 2-108
DS3: LPBKDS3FEAC-CMD, page 2-108
DS3: LPBKFACILITY (DS-1 or DS-3), page 2-109
DS3: LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110
DS3: RAI, page 2-135
DWDM Client: AIS, page 2-21
DWDM Client: AS-CMD, page 2-28
DWDM Client: AS-MT, page 2-29
DWDM Client: AUTOLSROFF, page 2-30
DWDM Client: CARLOSS (ML-Series), page 2-42
DWDM Client: FAILTOSW, page 2-65
DWDM Client: EOC, page 2-57
DWDM Client: FORCED-REQ-SPAN, page 2-81
DWDM Client: HI-LASERBIAS, page 2-83
DWDM Client: HI-LASERTEMP, page 2-84
DWDM Client: HI-RXPOWER, page 2-84
DWDM Client: HI-TXPOWER, page 2-86
DWDM Client: LOCKOUT-REQ, page 2-93
DWDM Client: LOF (OC-N), page 2-96
DWDM Client: LO-LASERBIAS, page 2-97
DWDM Client: LO-LASERTEMP, page 2-97
DWDM Client: LO-RXPOWER, page 2-99
DWDM Client: LO-TXPOWER, page 2-106
DWDM Client: LOS (OC-N), page 2-105
DWDM Client: LPBKFACILITY (OC-N), page 2-110
DWDM Client: LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110
DWDM Client: MANUAL-REQ-SPAN, page 2-113
DWDM Client: PORT-CODE-MISM, page 2-130
DWDM Client: PORT-COMM-FAIL, page 2-131
DWDM Client: PORT-MISMATCH, page 2-131
DWDM Client: PORT-MISSING, page 2-131
DWDM Client: RFI-L, page 2-136
DWDM Client: SD, page 2-139

Table 2-6   Alarm Index by Alarm Type (continued)

Table 2-6   Alarm Index by Alarm Type (continued)

DWDM Trunk: LO-RXTEMP, page 2-100
DWDM Trunk: LOS (OC-N), page 2-105
DWDM Trunk: LO-TXPOWER, page 2-106
DWDM Trunk: LPBKFACILITY (EC-N), page 2-109
DWDM Trunk: LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110
DWDM Trunk: ODUK-AIS-PM, page 2-119
DWDM Trunk: ODUK-BDI-PM, page 2-120
DWDM Trunk: ODUK-LCK-PM, page 2-120
DWDM Trunk: ODUK-OCI-PM, page 2-121
DWDM Trunk: ODUK-SD-PM, page 2-121
DWDM Trunk: ODUK-SF-PM, page 2-122
DWDM Trunk: ODUK-TIM-PM, page 2-122
DWDM Trunk: OTUK-AIS, page 2-123
DWDM Trunk: OTUK-BDI, page 2-123
DWDM Trunk: OTUK-IAE, page 2-124
DWDM Trunk: OTUK-LOF, page 2-124
DWDM Trunk: OTUK-SD, page 2-125
DWDM Trunk: OTUK-SF, page 2-125
DWDM Trunk: OTUK-TIM, page 2-125
DWDM Trunk: RFI-L, page 2-136
DWDM Trunk: SD, page 2-139
DWDM Trunk: SF, page 2-141
DWDM Trunk: SQUELCHED, page 2-146
DWDM Trunk: SSM-DUS, page 2-147
DWDM Trunk: SSM-FAIL, page 2-147
DWDM Trunk: SSM-LNC, page 2-147
DWDM Trunk: SSM-OFF, page 2-147
DWDM Trunk: SSM-PRC, page 2-148
DWDM Trunk: SSM-PRS, page 2-148
DWDM Trunk: SSM-RES, page 2-148
DWDM Trunk: SSM-SMC, page 2-148
DWDM Trunk: SSM-ST2, page 2-149
DWDM Trunk: SSM-ST3, page 2-149
DWDM Trunk: SSM-ST3E, page 2-149
DWDM Trunk: SSM-ST4, page 2-149
DWDM Trunk: SSM-STU, page 2-150
DWDM Trunk: SSM-TNC, page 2-150

Table 2-6   Alarm Index by Alarm Type (continued)

DWDM Trunk: TIM-P, page 2-155
DWDM Trunk: UNC-WORD, page 2-159
DWDM Trunk: WVL-MISMATCH, page 2-162
ECN: AIS-L, page 2-22
ECN: AS-CMD, page 2-28
ECN: AS-MT, page 2-29
ECN: LOF (EC-N), page 2-96
ECN: LOS (EC-N), page 2-103
ECN: LPBKFACILITY (DS-1 or DS-3), page 2-109
ECN: LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110
ECN: RFI-L, page 2-136
ENV: EXT, page 2-64
EQPT: AS-CMD, page 2-28
EQPT: AUTORESET, page 2-31
EQPT: BKUPMEMP, page 2-36
EQPT: CARLOSS (EQPT), page 2-37
EQPT: CLDRESTART, page 2-45
EQPT: COMIOXC, page 2-46
EQPT: CONTBUS-A-18, page 2-47
EQPT: CONTBUS-B-18, page 2-47
EQPT: CONTBUS-IO-A, page 2-48
EQPT: CONTBUS-IO-B, page 2-49
EQPT: CTNEQPT-PBPROT, page 2-50
EQPT: CTNEQPT-PBWORK, page 2-52
EQPT: ERROR-CONFIG, page 2-60
EQPT: EQPT, page 2-59
EQPT: EXCCOL, page 2-63
EQPT: FAILTOSW, page 2-65
EQPT: FORCED-REQ, page 2-80
EQPT: HITEMP, page 2-86
EQPT: IMPROPRMVL, page 2-87
EQPT: INHSWPR, page 2-89
EQPT: INHSWWKG, page 2-90
EQPT: LOCKOUT-REQ, page 2-93
EQPT: MAN-REQ, page 2-112
EQPT: MANRESET, page 2-112
EQPT: MEA (EQPT), page 2-115

Table 2-6   Alarm Index by Alarm Type (continued)

EQPT: MEM-GONE, page 2-117
EQPT: MEM-LOW, page 2-118
EQPT: NO-CONFIG, page 2-118
EQPT: PEER-NORESPONSE, page 2-128
EQPT: PROTNA, page 2-132
EQPT: PWR-REDUN, page 2-134
EQPT: RUNCFG-SAVENEED, page 2-139
EQPT: SFTWDOWN, page 2-143
EQPT: SWMTXMOD, page 2-150
EQPT: WKSWPR, page 2-162
EQPT: WTR, page 2-162
ETHER: AS-CMD, page 2-28
ETHER: CARLOSS (E-Series), page 2-38
ETHER: CARLOSS (G-Series), page 2-39
EXTSYNCH: FRCDSWTOPRI, page 2-81
EXTSYNCH: FRCDSWTOSEC, page 2-81
EXTSYNCH: FRCDSWTOTHIRD, page 2-82
EXTSYNCH: MANSWTOPRI, page 2-112
EXTSYNCH: MANSWTOSEC, page 2-113
EXTSYNCH: MANSWTOTHIRD, page 2-113
EXTSYNCH: SWTOPRI, page 2-152
EXTSYNCH: SWTOSEC, page 2-152
EXTSYNCH: SWTOTHIRD, page 2-152
EXTSYNCH: SYNCPRI, page 2-153
EXTSYNCH: SYNCSEC, page 2-154
EXTSYNCH: SYNCTHIRD, page 2-154
FAN: EQPT-MISS, page 2-60
FAN: FAN, page 2-70
FAN: FANDEGRADE, page 2-71
FAN: MEA (FAN), page 2-117
FAN: MFGMEM, page 2-118
FUDC: AIS, page 2-21
FUDC: LOS (OC-N), page 2-105
HDGE [G1000]: AS-CMD, page 2-28
HDGE [G1000]: AS-MT, page 2-29
HDGE [G1000]: CARLOSS (G-Series), page 2-39
HDGE [G1000]: LPBKTERMINAL (G-Series), page 2-111

Table 2-6   Alarm Index by Alarm Type (continued)

HDGE [G1000]: TPTFAIL (G-Series), page 2-156
ML1000: AS-CMD, page 2-28
ML1000: CARLOSS (ML-Series), page 2-42
ML1000: TPTFAIL (ML-Series), page 2-157
MSUDC: AIS, page 2-21
MSUDC: LOS (OC-N), page 2-105
NBR: RSVP-HELLODOWN, page 2-138
NE: AS-CMD, page 2-28
NE: AUD-LOG-LOSS, page 2-29
NE: AUD-LOG-LOW, page 2-30
NE: BAT-A-HGH-VLT, page 2-34
NE: BAT-A-LOW-VLT, page 2-35
NE: BAT-B-HGH-VLT, page 2-35
NE: BAT-B-LOW-VLT, page 2-35
NE: DATAFLT, page 2-53
NE: DBOSYNC, page 2-54
NE: EHIBATVG-A, page 2-56
NE: EHIBATVG-B, page 2-56
NE: ELWBATVG-A, page 2-56
NE: ELWBATVG-B, page 2-57
NE: HITEMP, page 2-86
NE: LAN-POL-REV, page 2-90
NE: PRC-DUPID, page 2-132
NE: PWR-A, page 2-133
NE: PWR-B, page 2-134
NE: SNTP-HOST, page 2-144
NE: SYSBOOT, page 2-155
NERING: BLSROSYNC, page 2-36
NERING: FULLPASSTHR-BI, page 2-82
NERING: KB-PASSTHR, page 2-90
NERING: PRC-DUPID, page 2-132
NERING: RING-MISMATCH, page 2-138
NESYNCH: FRCDSWTOINT, page 2-81
NESYNCH: FRCDSWTOPRI, page 2-81
NESYNCH: FRCDSWTOSEC, page 2-81
NESYNCH: FRCDSWTOTHIRD, page 2-82
NESYNCH: FRNGSYNC, page 2-82

Table 2-6   Alarm Index by Alarm Type (continued)

NESYNCH: FSTSYNC, page 2-82
NESYNCH: HLDOVRSYNC, page 2-87
NESYNCH: MANSWTOINT, page 2-112
NESYNCH: MANSWTOPRI, page 2-112
NESYNCH: MANSWTOSEC, page 2-113
NESYNCH: MANSWTOTHIRD, page 2-113
NESYNCH: SSM-PRS, page 2-148
NESYNCH: SSM-RES, page 2-148
NESYNCH: SSM-SMC, page 2-148
NESYNCH: SSM-ST2, page 2-149
NESYNCH: SSM-ST3, page 2-149
NESYNCH: SSM-ST3E, page 2-149
NESYNCH: SSM-ST4, page 2-149
NESYNCH: SSM-STU, page 2-150
NESYNCH: SSM-TNC, page 2-150
NESYNCH: SWTOPRI, page 2-152
NESYNCH: SWTOSEC, page 2-152
NESYNCH: SWTOTHIRD, page 2-152
NESYNCH: SYNCPRI, page 2-153
NESYNCH: SYNCSEC, page 2-154
NESYNCH: SYNCTHIRD, page 2-154
OCN: AIS-L, page 2-22
OCN: APSB, page 2-23
OCN: APSCDFLTK, page 2-24
OCN: APSC-IMP, page 2-24
OCN: APSCINCON, page 2-25
OCN: APSCM, page 2-25
OCN: APSCNMIS, page 2-26
OCN: APSMM, page 2-27
OCN: AS-CMD, page 2-28
OCN: AS-MT, page 2-29
OCN: AUTOLSROFF, page 2-30
OCN: EOC, page 2-57
OCN: E-W-MISMATCH, page 2-61
OCN: EXERCISE-RING-REQ, page 2-64
OCN: EXERCISE-SPAN-REQ, page 2-64
OCN: EXTRA-TRAF-PREEMPT, page 2-65

Table 2-6   Alarm Index by Alarm Type (continued)

OCN: FAILTOSW, page 2-65
OCN: FAILTOSWR, page 2-67
OCN: FAILTOSWS, page 2-68
OCN: FE-EXERCISING-RING, page 2-75
OCN: FE-FRCDWKSWPR-SPAN, page 2-76
OCN: FE-FRCDWKSWPR-RING, page 2-75
OCN: FORCED-REQ-SPAN, page 2-81
OCN: FE-LOCKOUTOFPR-SPAN, page 2-77
OCN: FE-MANWKSWPR-RING, page 2-78
OCN: FE-MANWKSWPR-SPAN, page 2-79
OCN: FEPRLF, page 2-79
OCN: FORCED-REQ-RING, page 2-80
OCN: FORCED-REQ-SPAN, page 2-81
OCN: LASEREOL, page 2-91
OCN: LKOUTPR-S, page 2-91
OCN: LOCKOUT-REQ, page 2-93
OCN: LOCKOUT-REQ-RING, page 2-93
OCN: LOF (OC-N), page 2-96
OCN: LOS (OC-N), page 2-105
OCN: LPBKFACILITY (OC-N), page 2-110
OCN: LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N), page 2-110
OCN: MANUAL-REQ-RING, page 2-113
OCN: MANUAL-REQ-SPAN, page 2-113
OCN: RFI-L, page 2-136
OCN: RING-SW-EAST, page 2-138
OCN: RING-SW-WEST, page 2-138
OCN: SD-L, page 2-140
OCN: SF-L, page 2-142
OCN: SPAN-SW-EAST, page 2-144
OCN: SPAN-SW-WEST, page 2-144
OCN: SQUELCH, page 2-145
OCN: SSM-DUS, page 2-147
OCN: SSM-FAIL, page 2-147
OCN: SSM-OFF, page 2-147
OCN: SSM-PRS, page 2-148
OCN: SSM-RES, page 2-148
OCN: SSM-SMC, page 2-148

Table 2-6   Alarm Index by Alarm Type (continued)

OCN: SSM-ST2, page 2-149
OCN: SSM-ST3, page 2-149
OCN: SSM-ST3E, page 2-149
OCN: SSM-ST4, page 2-149
OCN: SSM-STU, page 2-150
OCN: SSM-TNC, page 2-150
OCN: SYNC-FREQ, page 2-153
OCN: WKSWPR, page 2-162
OCN: WTR, page 2-162
STSMON: AIS-P, page 2-22
STSMON: AUTOSW-AIS, page 2-31
STSMON: AUTOSW-LOP (STSMON), page 2-32
STSMON: AUTOSW-PDI, page 2-32
STSMON: AUTOSW-SDBER, page 2-33
STSMON: AUTOSW-SFBER, page 2-33
STSMON: AUTOSW-UNEQ (STSMON), page 2-34
STSMON: FAILTOSW-PATH, page 2-66
STSMON: FORCED-REQ, page 2-80
STSMON: LOCKOUT-REQ, page 2-93
STSMON: LOP-P, page 2-98
STSMON: LPBKCRS, page 2-107
STSMON: MAN-REQ, page 2-112
STSMON: PDI-P, page 2-126
STSMON: PLM-P, page 2-128
STSMON: RFI-P, page 2-136
STSMON: SD-P, page 2-141
STSMON: SF-P, page 2-142
STSMON: TIM-P, page 2-155
STSMON: UNEQ-P, page 2-159
STSMON: WKSWPR, page 2-162
STSMON: WTR, page 2-162
STSTERM: AIS-P, page 2-22
STSTERM: LOP-P, page 2-98
STSTERM: PDI-P, page 2-126
STSTERM: PLM-P, page 2-128
STSTERM: RFI-P, page 2-136
STSTERM: SD-P, page 2-141

Table 2-6   Alarm Index by Alarm Type (continued)

STSTERM: SF-P, page 2-142
STSTERM: TIM-P, page 2-155
STSTERM: UNEQ-P, page 2-159
VT-MON: AIS-V, page 2-22
VT-MON: AUTOSW-AIS, page 2-31
VT-MON: AUTOSW-LOP (VTMON), page 2-32
VT-MON: AUTOSW-UNEQ (VTMON), page 2-34
VT-MON: FAILTOSW-PATH, page 2-66
VT-MON: FORCED-REQ, page 2-80
VT-MON: LOCKOUT-REQ, page 2-93
VT-MON: LOP-V, page 2-99
VT-MON: MAN-REQ, page 2-112
VT-MON: UNEQ-V, page 2-161
VT-MON: WKSWPR, page 2-162
VT-MON: WTR, page 2-162
VT-TERM: AIS-V, page 2-22
VT-TERM: PLM-V, page 2-130
VT-TERM: RFI-V, page 2-137
VT-TERM: SD-P, page 2-141
VT-TERM: SF-P, page 2-142
VT-TERM: UNEQ-V, page 2-161

2.3.1 Alarm Type/Object Definition

The following table defines abbreviations used in the alarm troubleshooting procedures.

Table 2-7   Alarm Type/Object Definition

AEP	Alarm expansion panel
AIP	Auxiliary interface protection module
BITS	Building integration timing supply (BITS) incoming references (BITS-1, BITS-2)
BP	The backplane
CC	Unified control plane (UCP) communication channel
CKT	UCP circuit
DS1	A DS-1 line a DS-1 card
DS3	A DS-3 line on a DS-3 card
ECN	An EC-N line on an EC-N card
DWDM Client	The port (such as OC-12 or OC-48) where the client signal is plugged in

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

DWDM Trunk	The main span of the link; from the card point of view, it is the port operating in the 100-GHz spacing frequency grid
ENV	An environmental alarm port
EQPT	A card in any of the 8 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
ETHER	Ethernet, such as for straight-through (CAT-5) LAN cables
EXTSYNCH	BITS outgoing references (SYNC-BITS1, SYNC-BITS2)
FAN	Fan-tray assembly
FUDC	SONET F1 byte user data channel
HDGE	High Density Gigabit Ethernet; applies to G1000-4 cards.
ML1000	ML-Series Ethernet (traffic) cards
MSUDC	SONET Multiplex Section User Data Channel
NBR	UCP neighbor
NE	The entire network element
NERING	Represents the ring status in the NE
NE-SYNCH	Represents the timing status of the NE
OCN	An OC-N line on an OC-N card
STSMON	STS alarm detection at the monitor point (upstream from the cross-connect)
STSTERM	STS alarm detection at termination (downstream from the cross-connect)
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 Trouble Notifications

The ONS 15454 uses standard Telcordia categories to characterize levels of trouble. The ONS 15454 reports alarmed trouble notifications in the CTC Alarms window and Not Alarmed (NA) trouble notifications in the Conditions window. Alarms signify a problem that the user needs to fix, such as an LOS (OC-N). Conditions notify the user of an event which does not require action, such as a SWTOSEC or a MANRESET.

Telcordia further divides alarms into Service-Affecting (SA) and NSA status. An SA failure affects a provided service or the network's ability to provide service. For example, a TRMT is characterized as an SA failure. TRMT-MISS occurs when the cable connector leading to a port on an active DS-1 card is removed. This affects a provided service because traffic switches to the protect card. HITEMP means that the alarm object is hotter than 122 degrees Fahrenheit (50 degrees Celsius). HITEMP is an NSA failure for a single piece of equipment, or an SA failure for the NE. For example, if the HITEMP alarm is raised against a port with an EQPT object, the alarm is NSA because port and card traffic is protected. If the HITEMP alarm is raised against the NE (shelf), however, it is an SA alarm because a high temperature affects the network's ability to provide service.

2.4.1 Conditions

When an SA failure is detected, the ONS 15454 also sends an AIS downstream. When it receives the AIS, the receiving node sends an RFI-L upstream. AIS-L and RFI belong in the conditions category and show in the Conditions window of CTC. However, unlike most conditions which are Not Alarmed (NA), Telcordia classifies these conditions as Not Reported (NR).

Both CTC and TL1 report NRs and NAs as conditions when conditions are retrieved. NAs are also reported as autonomous events in TL1 and in the History window of CTC. For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 and Cisco ONS 15327 TL1 Command Guide*.

2.4.2 Severities

The ONS 15454 uses Tecordia standard severities: Critical (CR), Major (MJ), and Minor (MN). Critical indicates a severe, service-affecting alarm that needs immediate correction. Major is a serious alarm, but the failure has less of an impact on the network. For example, with an LOS (DS-1), a Major alarm, 24 DS-0 circuits lose protection. But with a LOS (OC-N) for an OC-192 card, a Critical alarm, over one hundred thousand DS-0 circuits lose protection.

Minor alarms, such as FSTSYNC, do not have a serious affect on service. FSTSYNC lets you know that the ONS 15454 is choosing a new timing reference because the old reference failed. The loss of the prior timing source is something a user needs to look at, but it should not immediately disrupt service.

Telcordia standard severities are the default settings for the ONS 15454. A user may 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 alarm severity for the active reporting card, if applicable. The default severity for alarms reported by standby cards is always Minor, Non-Service-Affecting.

2.5 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 and warnings:

⚠ **Caution**   Hazardous voltage or energy might 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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Warning   **Class 1 laser product.**

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

2.6 Alarm Procedures

This section list 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're done checking for alarms, click the alarm filter icon again to turn filtering back on.

Note   When checking alarms, make sure that alarm suppression is not enabled on the card or port. For more information about alarm suppression, see the *Cisco ONS 15454 Procedure Guide*.

2.6.1 AIS

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

The Alarm Indication Signal (AIS) condition in the SONET overhead is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service (IS) but the DS-3 or OC-N port on a node upstream on the circuit is not in service. The upstream node often reports a loss of service or has an out-of-service (OOS) port. The AIS clears when you clear the primary alarm on the upstream node. However, the primary alarm node might not report any alarms that indicate it is at fault.

Procedure: Clear the AIS Condition

Step 1   Verify whether there are alarms on the upstream nodes and equipment, especially an LOS (OC-N), page 2-105, or OOS ports.

Step 2   Clear the upstream alarms using the applicable procedure(s) in this chapter.

Step 3   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.2 AIS-L

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

The AIS Line condition means there is an error in the SONET overhead at the line layer. The AIS-L condition is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service (IS) but a node upstream on the circuit does not have its OC-N port in service. The upstream node often reports an LOS or has an OOS port. The AIS-L clears when you clear the primary alarm on the upstream node. However, the primary alarm node might not report any alarms that indicate it is at fault.

Procedure: Clear the AIS-L Condition

Step 1   Complete the "Clear the AIS Condition" procedure on page 2-21.

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

2.6.3 AIS-P

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

The AIS Path condition means there is an error in the SONET overhead at the path layer. The AIS-P condition is secondary to another alarm occurring simultaneously in an upstream node. The AIS is caused by an incomplete circuit path, for example, when the port on the reporting node is in service (IS), but a node upstream on the circuit does not have its port in service. The upstream node often reports an LOS (OC-N), page 2-105, or has an out of service (OOS) OC-N port. The AIS-P clears when the primary alarm on the upstream node is cleared. However, the node with the primary alarm might not report any alarms to indicate it is at fault. AIS-P occurs at each node on the incoming OC-N path.

Procedure: Clear the AIS-P Condition

Step 1   Complete the "Clear the AIS Condition" procedure on page 2-21.

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

2.6.4 AIS-V

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

The AIS Virtual Tributary (VT) condition means there is an error in the SONET overhead at the VT layer. The AIS-V condition is secondary to another alarm occurring simultaneously in an upstream node. An incomplete circuit path causes an AIS, for example, when the port on the reporting node is in service (IS) but a node upstream on the circuit does not have its OC-N port in service. The upstream node often reports an LOS (OC-N), page 2-105, or has an out of service (OOS) port. The AIS-V clears when the primary alarm is cleared. The node with the OOS port might not report any alarms to indicate it is at fault.

An AIS-V error message on the electrical card is accompanied by an AIS-P, page 2-22, on the cross connected OC-N card.

Note   See the "AIS-V on DS3XM-6 Unused VT Circuits" section on page 1-71.

Procedure: Clear the AIS-V Condition

Step 1   Complete the "Clear the AIS Condition" procedure on page 2-21.

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

2.6.5 APSB

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

The Automatic Protection Switching (APS) Channel Byte Failure alarm occurs when line terminating equipment detects protection switching byte failure in the incoming APS signal. The failure occurs when an inconsistent APS byte or invalid code is detected. 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.

Procedure: 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 might not interoperate effectively with the ONS 15454.

Step 2   If the alarm does not clear and the overhead shows inconsistent or invalid K bytes, you might need to replace the upstream cards for protection switching to operate properly.

Caution   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

2.6.6 APSCDFLTK

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

The APS Default K Byte Received 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 configuration. A node in a path protection configuration 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 BLSROSYNC, page 2-36.

Procedure: Clear the APSCDFLTK Alarm

Step 1   Complete the "Identify a Ring ID or Node ID Number" procedure on page 2-164 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 Node ID Number" procedure on page 2-164 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" section on page 2-61.) 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, make sure 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 2-165.

Step 7   If nodes are not visible, complete the "Verify or Create Node DCC Terminations" procedure on page 2-165 to ensure that SONET DCC terminations exist on each node.

Step 8   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.7 APSC-IMP

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

An Improper SONET APS Code alarm indicates 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. APSCIMP occurs when these bits indicate a bad or invalid K byte. 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.

Procedure: 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 ID that matches the other node ring IDs. Complete the "Identify a Ring ID or Node ID Number" procedure on page 2-164.

Step 3   Repeat Step 2 for all nodes in the ring.

Step 4   If a node has a ring ID number that does not match the other nodes, make the ring ID number of that node identical to the other nodes. Complete the "Change a Ring ID Number" procedure on page 2-164.

Step 5   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.8 APSCINCON

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

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

Procedure: Clear the APSCINCON Alarm

Step 1   Look for other alarms, especially LOS (OC-N), page 2-105; LOF (OC-N), page 2-96, or AIS, page 2-21. Clearing these alarms clears the APSCINCON alarm.

Step 2   If an APSINCON alarm occurs with no other alarms, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.9 APSCM

• Major (MJ), Service Affecting (SA)

The APS Channel Mismatch 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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might 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.

Procedure: 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.10 APSCNMIS

- Major (MJ), Service Affecting (SA)

The APS Node ID Mismatch alarm occurs when the source node ID contained in the K2 byte of the incoming APS channel is not present in the ring map. The APSCNMIS alarm might 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.

Procedure: Clear the APSCNMIS Alarm

Step 1 Complete the "Identify a Ring ID or Node ID Number" procedure on page 2-164 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 Node ID Number" procedure on page 2-164 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 lock out 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 2-165 to lock out the span.

Step 6 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165 to clear the lock out.

Step 7 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.11 APSMM

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

An APS Mode Mismatch 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.

Procedure: Clear the APSMM Alarm

Step 1 For the reporting ONS 15454, display the node view and verify the protection scheme provisioning.

a. Click the **Provisioning > Protection** tabs.

b. Choose 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.

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/tac for more information or call TAC
(1-800-553-2447).

2.6.12 AS-CMD

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

The Alarms Suppressed by User Command condition applies to the network element (NE, or node),
backplane, and cards. It occurs when alarms are suppressed for one or more cards or for the entire shelf.

Procedure: Clear the AS-CMD Condition

Step 1   In the 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, 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 a "system," go to Step 8.

Step 3   If the AS-CMD condition is reported for a card, determine whether alarms are suppressed for a port and
if so, raise the suppressed alarms:

   a. Double-click the card to display the card view.

   b. Click the **Provisioning > Alarm 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   In node view, if the AS-CMD condition is reported for a card and not an individual port, click the
Provisioning > Alarm Behavior tabs.

Step 5   Locate the row for the reported card slot. (The slot number information was in the Object column in the
Conditions window that you noted in Step 2.)

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:

   a. In node view, click the **Provisioning > Alarm Behavior** tabs.

   b. In the Backplane row, deselect the Suppress Alarms column check box.

   c. Click **Apply**.

Step 8   If the condition is reported for the shelf, cards and other equipment are affected. To clear the alarm:

   a. In node view, click the **Provisioning > Alarm Behavior** tabs.

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

   c. Click **Apply**.

Step 9   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC
(1-800-553-2447).

2.6.13 AS-MT

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

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

Procedure: Clear the AS-MT Condition

Step 1   Complete the "Clear a Loopback" procedure on page 2-167.

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

2.6.14 AUD-LOG-LOSS

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

The Audit Trail Log Loss condition occurs when the log is 100% full and that the oldest entries are being
replaced as new entries are generated. The log capacity is 640 entries.

Procedure: Clear the AUD-LOG-LOSS Condition

Step 1   In the 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/tac for more information or call TAC
(1-800-553-2447).

2.6.15 AUD-LOG-LOW

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

The Audit Trail Log Loss condition occurs when the audit trail log is 80% full.

✎

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

2.6.16 AUTOLSROFF

- Critical (CR), Service Affecting (SA)

The Auto Laser Shutdown alarm occurs when the OC-192 card temperature exceeds 194° F (90 ° 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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Procedure: Clear the AUTOLSROFF Alarm

Step 1 View the temperature displayed on the ONS 15454 LCD front panel. For an illustration of the LCD panel, refer to the "View Alarm Counts on the LCD for a Slot or Port" procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 2 If the temperature of the shelf exceeds 194° F (90° C), the alarm should clear if you solve the ONS 15454 temperature problem. Complete the "Clear the HITEMP Alarm" procedure on page 2-86.

Step 3 If the temperature of the shelf is under 194° F (90° C), the HITEMP alarm is not the cause of the AUTOLSROFF alarm. Complete the "Physically Replace a Card" procedure on page 2-169 for the OC-192 card.

⚠

Caution Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

✎

Note When replacing a card with an identical type of card, no additional CTC provisioning is required.

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

2.6.17 AUTORESET

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

The Automatic System Reset 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.

Procedure: Clear the AUTORESET Alarm

Step 1   Verify that additional alarms that might have triggered an automatic reset.

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 2-169.

⚠️
Caution   Removing a card that currently caries 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. Consult 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 3   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.18 AUTOSW-AIS

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

The Automatic path protection configuration Switch Caused by AIS condition indicates that automatic path protection configuration protection switching occurred because of an AIS condition. The path protection configuration is configured for revertive switching and reverts to the working path after the fault clears.

Procedure: Clear the AUTOSW-AIS Condition

Step 1   Complete the "Clear the AIS Condition" procedure on page 2-21.

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

2.6.19 AUTOSW-LOP (STSMON)

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

The Automatic path protection configuration Switch Caused by Loss of Pointer (LOP) condition indicates that automatic path protection configuration protection switching occurred because of an LOP-P, page 2-98. The path protection configuration is configured for revertive switching and reverts to the working path after the fault clears.

Procedure: Clear the AUTOSW-LOP (STSMON) Condition

Step 1   Complete the "Clear the LOP-P Alarm" procedure on page 2-98.

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

2.6.20 AUTOSW-LOP (VTMON)

- Minor (MN), Service Affecting (SA)

The AUTOSW-LOP alarm indicates that automatic path protection configuration protection switching occurred because of an LOP-V, page 2-99. The path protection configuration is configured for revertive switching and reverts to the working path after the fault clears.

Procedure: Clear the AUTOSW-LOP (VTMON) Alarm

Step 1   Complete the "Clear the LOP-V Alarm" procedure on page 2-99.

Step 2   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.21 AUTOSW-PDI

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

The Automatic path protection configuration Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic path protection configuration protection switching occurred because of a PDI-P, page 2-126. The path protection configuration is configured for revertive switching and reverts to the working path after the fault clears.

Procedure: Clear the AUTOSW-PDI Condition

Step 1   Complete the "Clear the PDI-P Condition" procedure on page 2-127.

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

2.6.22 AUTOSW-SDBER

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

The Automatic path protection configuration Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that a signal degrade [SD, page 2-139] caused automatic path protection configuration protection switching to occur. The path protection configuration is configured for revertive switching and reverts to the working path when the SD is resolved.

Procedure: Clear the AUTOSW-SDBER Condition

Step 1   Complete the "Clear the SD Condition" procedure on page 2-140.

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

2.6.23 AUTOSW-SFBER

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

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a signal fail SF, page 2-141, caused automatic path protection configuration protection switching to occur. The path protection configuration is configured for revertive switching and reverts to the working path when the SF is resolved.

Procedure: Clear the AUTOSW-SFBER Condition

Step 1   Complete the "Clear the SF Condition" procedure on page 2-142.

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

2.6.24 AUTOSW-UNEQ (STSMON)

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

The Automatic path protection configuration Switch Caused by Unequipped (UNEQ-P, page 2-159), indicates that an UNEQ alarm caused automatic path protection configuration protection switching to occur. The path protection configuration is configured for revertive switching and reverts to the working path after the fault clears.

Procedure: Clear the AUTOSW-UNEQ (STSMON) Condition

Step 1   Complete the "Clear the UNEQ-P Alarm" procedure on page 2-159.

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

2.6.25 AUTOSW-UNEQ (VTMON)

- Minor (MN), Service Affecting (SA)

AUTOSW-UNEQ (VTMON) indicates that an UNEQ-V alarm caused automatic path protection configuration protection switching to occur. The path protection configuration is configured for revertive switching and reverts to the working path after the fault clears.

Procedure: Clear the AUTOSW-UNEQ (VTMON) Alarm

Step 1   Complete the "Clear the UNEQ-V Alarm" procedure on page 2-161.

Step 2   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.26 BAT-A-HGH-VLT

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

The High Voltage Battery (BAT) A condition occurs when the voltage level on battery lead A is between –52 VDC and –56.7 VDC. The condition indicates that the voltage on the battery lead is high. The condition remains until the voltage remains under this range for 120 seconds.

Procedure: Clear the BAT-A-HGH-VLT Condition

Step 1   The problem is external to the ONS 15454. Troubleshoot the power source supplying battery lead A.

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

2.6.27 BAT-A-LOW-VLT

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

The Low Voltage Battery A condition occurs when the voltage on battery feed A is low. The low voltage battery A condition occurs when the voltage on battery feed A is between –44 VDC and –40 VDC. The condition clears when voltage remains above this range for 120 seconds.

Procedure: Clear the BAT-A-LOW-VLT Condition

Step 1   The problem is external to the ONS 15454. Troubleshoot the power source supplying battery lead A.

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

2.6.28 BAT-B-HGH-VLT

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

The High Voltage Battery B condition occurs when the voltage level on battery lead B is between –52 VDC and –56.7 VDC. The condition indicates that the voltage on the battery lead is high. The condition remains until the voltage remains under this range for 120 seconds.

Procedure: Clear the BAT-B-HGH-VLT Condition

Step 1   The problem is external to the ONS 15454. Troubleshoot the power source supplying battery lead B.

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

2.6.29 BAT-B-LOW-VLT

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

The Low Voltage Battery B condition occurs when the voltage level on battery lead B is between –44 VDC and –40 VDC. The condition indicates that the voltage on the battery lead is high. The condition remains until the voltage remains under this range for 120 seconds.

Procedure: Clear the BAT-B-LOW-VLT Condition

Step 1   The problem is external to the ONS 15454. Troubleshoot the power source supplying battery lead B.

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

2.6.30 BKUPMEMP

- Critical (CR), Non-Service Affecting (NSA)

The Primary Non-Volatile Backup Memory Failure alarm refers to a problem with the TCC+/TCC2 card's flash memory. The alarm occurs when the TCC+/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 TCC+/TCC2.

The BKUPMEMP alarm can also cause an EQPT alarm. 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 TCC+/TCC2 card.

Procedure: Clear the BKUPMEMP Alarm

Step 1   Verify that both TCC+/TCC2 cards are powered and enabled by confirming lighted ACT/STBY LEDs on the TCC+/TCC2 cards.

Step 2   If both TCC+/TCC2 cards are powered and enabled, reset the active TCC+/TCC2 card to make the standby TCC+/TCC2 card active. Complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

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

Step 3   If the TCC+/TCC2 you reset does not reboot 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 TCC+/TCC2" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

2.6.31 BLSROSYNC

- Major (MJ), Service Affecting (SA)

The BLSR Out Of Synchronization alarm is caused 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.

Procedure: Clear the BLSROSYNC Alarm

Step 1   Reestablish cabling continuity to the node reporting the alarm.

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 2-57.

Step 3   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.32 CARLOSS (EQPT)

- Major (MJ), Service Affecting (SA)

A Carrier Loss on the LAN Equipment alarm occurs 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 TCC+/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.

Procedure: Clear the CARLOSS (EQPT) Alarm

Step 1   Verify connectivity by pinging the ONS 15454 that is reporting the alarm:

   a.   If you are using a Microsoft Windows operating system, from the Start Menu choose **Programs > Accessories > Command Prompt**.

   b.   If you are using a Sun Solaris operating system, from the Common Desktop Environment (CDE) click the **Personal Application** tab and click **Terminal**.

   c.   For both the Sun and Microsoft operating systems, at the prompt type:

   ping [ONS 15454 IP address]

   For example, ping 192.1.0.2.

   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 2   If the ping is successful, an active TCP/IP connection exists. Restart CTC:

   a.   Exit from CTC.

   b.   Reopen the browser.

   c.   Log into CTC.

Step 3   Verify that the straight-through (CAT-5) LAN cable is properly connected and attached to the correct port.

Step 4   If the straight-through (CAT-5) LAN 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 5   If you are unable to establish connectivity, replace the straight-through cable with a new known-good cable.

Step 6   If you are unable to establish connectivity, perform standard network or LAN diagnostics. For example, trace the IP route, verify cables continuity, and troubleshoot any routers between the node and CTC.

Step 7   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.33 CARLOSS (E-Series)

- Major (MJ), Service Affecting (SA)

A Carrier Loss alarm on the LAN E-Series Ethernet (traffic) card is the data equivalent of an LOS (OC-N), page 2-105. 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 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.

Procedure: Clear the CARLOSS (E-Series) Alarm

Step 1   Verify that the straight-through (CAT-5) LAN cable is properly connected and attached to the correct port.

Step 2   If the straight-through (CAT-5) LAN 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 straight-through (CAT-5) LAN 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 2-170 for the Ethernet (traffic) card.

Step 7   If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the Ethernet card.

⚠️

Caution   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

✎

Note   When replacing a card with an identical type of card, no additional CTC provisioning is required.

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.

Step 9   If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, then the reappearing alarm might 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 the **Select Affected Circuits** dialog box 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 2-167 and reconfigure the circuit with the correct circuit size. For more information, refer to the *Cisco ONS 15454 Procedure Guide*.

Step 10   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.34 CARLOSS (G-Series)

   •   Major (MJ), Service Affecting (SA)

A Carrier Loss alarm on the LAN G-Series Ethernet (traffic) card is the data equivalent of an LOS (OC-N), page 2-105. 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 TPTFAIL (G-Series), page 2-156, 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" section on page 2-158 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.

Procedure: Clear the CARLOSS (G-Series) Alarm

Step 1   Verify that the straight-through (CAT-5) LAN cable is properly connected and attached to the correct port.

Step 2   If the straight-through (CAT-5) LAN 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   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 5   If a valid Ethernet signal is not present and the transmitting device is operational, replace the straight-through (CAT-5) LAN cable connecting the transmitting device to the Ethernet port.

Step 6   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, verify 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 7   If the alarm does not clear, disable and reenable the Ethernet port to attempt to remove the CARLOSS condition. (The autonegotiation process restarts.)

Step 8   If the alarm does not clear and a TPTFAIL (G-Series) is also reported, complete the "Clear the TPTFAIL (G-Series) Alarm" procedure on page 2-157. 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 might be the G1000-4's end-to-end link integrity feature taking action on a remote failure indicated by the TPTFAIL alarm.

Step 9   If the TPTFAIL alarm was not reported, verify whether a terminal loopback has been provisioned on the port:

    a. In the node view, click the card to go to card view.

    b. Click the **Conditions** tab and the **Retrieve Conditions** button.

    c. If LPBKTERMINAL is listed for the port, a loopback is provisioned. Go to Step 10. If IS is listed, go to Step 11.

Step 10   If a loopback was provisioned, complete the "Clear a Loopback" procedure on page 2-167.

On the G1000-4 card, provisioning a terminal 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 11.

Step 11   If a CARLOSS alarm repeatedly appears and clears, the reappearing alarm might 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 OSI/TARP-based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.

    a. Right-click anywhere in the row of the CARLOSS alarm.

    b. Right-click or left-click the **Select Affected Circuits** dialog box.

    c. Record the information in the type and size columns of the highlighted circuit.

    d. Examine the layout of your network and determine which ONS 15454 and card host the Ethernet circuit at the other end of the Ethernet manual cross-connect.

       • 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.

    e. Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.

    f. If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-167 and reconfigure the circuit with the correct circuit size. Refer to the *Cisco ONS 15454 Procedure Guide* for detailed procedures to create circuits.

Step 12   If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170.

Step 13   If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the Ethernet card.

⚠

Caution   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

✎

Note   When replacing a card with an identical type of card, no additional CTC provisioning is required.

Step 14   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.35 CARLOSS (ML-Series)

- Major (MJ), Service Affecting (SA)

A Carrier Loss alarm on the ML-series Ethernet (traffic) card is the data equivalent of an LOS (OC-N), page 2-105. The Ethernet port has lost its link and is not receiving a valid signal.

A CARLOSS alarm is caused when the Ethernet port has been configured from the internal operating system (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*.

Procedure: Clear the CARLOSS (ML-Series) 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 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 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, perform a facility loopback on the ML card. Complete the "Perform a Facility Loopback on a Source DS-N Port" procedure on page 1-5.

Step 7   If the problem persists with the loopback installed, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168.

Step 8   If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169.

⚠

Caution   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

✎

Note   When replacing a card with an identical type of card, no additional CTC provisioning is required.

Step 9   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.36 CKTDOWN

 • Critical (CR), Service Affecting (SA)

The UCP Circuit Down alarm applies to logical circuits created within the UCP between devices. It occurs when the 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.

Procedure: Clear the CKTDOWN Alarm

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

 a.   In the node view, click the **Provisioning > UCP > Neighbor** tabs.

 b.   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.

 c.   Click **Start > Programs > Accessories > Command Prompt** to open an MS-DOS command window for pinging the neighbor.

 d.   At the command prompt (C:\>), type:

```
ping [node DNS name or 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.

   e. 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**.

   f. If the ping was unsuccessful, you will get the following reply repeated 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 channel to neighbor has not been provisioned, or if you had to delete the channel, create one:

   a. In the Provisioning > UCP > Neighbor tabs, click the **Create** button.

   b. 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.

   c. 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 will say 0.0.0.0.

Step 3 If neighbor discovery is enabled, make sure that the neighbor node ID, remote 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.

   a. Click the entry to select the neighbor IP address and click **Delete**.

   b. If you get an error that will not allow you to delete the IPCC, you will have to delete the neighbor and recreate it. Click the **Neighbor** tab.

   c. Click to select the neighbor and click **Delete**.

   d. Then 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:

   a. In the Provisioning > UCP > IPCC tabs, click **Create**.

   b. In the Unified Control Plane Provisioning window, click **Next**.

   c. If no IPCCs are listed, click **Create**.

   d. In the Create New IPCC window, click one of the DCC terminations in the DCC list.

Leave the SDCC radio button selected (as long as DCCs have been created on the node) and leave the Leave Unchanged radio button selected.

   e. Click **OK**. The IPCC is listed as CCID 1 in the Unified Control Plane Provisioning window.

f. Click the neighbor to select it, and click **Next**.

g. Choose a UCP interface (for example Slot 5 (OC48), port 1) from the pull-down menu. The field default is the node where you are logged in.

h. Choose the UCP interface TNA address type. The default is IPv4. The address field lists the login node IP address by default.

i. 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:

a. Click the **Interface** tab. View the slot and port listed in the Interface column (for example, Slot 5 (OC48), port 1).

b. 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.37 CLDRESTART

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

The Cold Restart 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.

Procedure: Clear the CLDRESTART Condition

Step 1 If the condition fails to clear after the card reboots, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168.

Step 2 If the condition does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the card.

⚠

Caution   Removing a card that currently caries 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. Consult 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 3   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.38 COMIOXC

*   Critical (CR), Service Affecting (SA)

The Input/Output Slot To Cross-Connect Communication Failure alarm is caused by the cross-connect card. It occurs when there is a communication failure for a traffic (multispeed slots or high-speed) slot.

Procedure: Clear the COMIOXC Alarm

Step 1   Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 on the reporting cross-connect card.

*   While the card resets, the FAIL LED on the physical card blinks and turns off.

*   While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 2   Verify that the reset is complete and error-free.

*   No new alarms appear in the Alarms window in CTC.

*   If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.

*   If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

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 Cross-Connect Cards" procedure on page 2-166.

Step 4   Complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the reporting cross-connect card.

Step 5   If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.39 CONTBUS-A-18

- Major (MJ), Non-Service Affecting (NSA)

A Communication Failure from TCC+/TCC2 Slot to TCC+/TCC2 Slot alarm occurs when the main processor on the TCC+/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 TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168 to make the TCC+/TCC2 in Slot 11 active.

Step 2 Wait approximately 10 minutes for the TCC+/TCC2 in Slot 7 to reset as the standby TCC+/TCC2. Verify that the standby LED is illuminated before proceeding to the next step.

Step 3 Position the cursor over the TCC+/TCC2 card in Slot 11 and complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168 to make the standby TCC+/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 TCC+/TCC2" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

2.6.40 CONTBUS-B-18

- Major (MJ), Non-Service Affecting (NSA)

A Communication Failure from TCC+/TCC2 Slot to TCC+/TCC2 Slot alarm occurs when the main processor on the TCC+/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 TCC+/TCC2 card in Slot 11 and complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168 to make the TCC+/TCC2 in Slot 7 active.

Step 2 Wait approximately 10 minutes for the TCC+/TCC2 in Slot 11 to reset as the standby TCC+/TCC2. Verify that the standby LED is illuminated before proceeding to the next step.

Step 3 Position the cursor over the TCC+/TCC2 card in Slot 7 and complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168 to make the standby TCC+/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 TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

2.6.41 CONTBUS-IO-A

- Major (MJ), Non-Service Affecting (NSA)

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

This alarm can also appear when you upgrade from TCC+ cards to TCC2 cards. In this case, it clears without intervention within about 13 minutes.

⚠ **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 (BP) alarm (see page 2-114) for the reporting card.

Step 2 If the alarm object is any single card slot other than the standby TCC+/TCC2 in Slot 11, perform a CTC reset of the object card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-169. Verify that the following LED behavior takes place:

- While the card resets, the FAIL LED on the physical card blinks and turns off.
- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 3   If the alarm object is the standby TCC+/TCC2 in Slot 11, perform a soft reset of this card:

    a.   Right-click the Slot 11 TCC+/TCC2 card.

    b.   Choose **Reset Card** from the shortcut menu.

    c.   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 TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

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. Verify that the SBY LED is blinking on the standby card.

Step 6   If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the reporting card.

Step 7   If the reseated 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 TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

2.6.42 CONTBUS-IO-B

- Major (MJ), Non-Service Affecting (NSA)

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

This alarm can also appear when you upgrade from TCC+ cards to TCC2 cards. In this case, it clears without intervention within about 13 minutes.

⚠
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 (BP) alarm (see page 2-114) for the reporting card.

Step 2 If the alarm object is any single card slot other than the standby TCC+/TCC2 in Slot 7, perform a CTC reset of the object card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-169. Verify that the following LED behavior takes place:

- While the card resets, the FAIL LED on the physical card blinks and turns off.

- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 3 If the alarm object is the standby TCC+/TCC2 in Slot 7, perform a soft reset of this card:

    a. Right-click the Slot 7 TCC+/TCC2 card.

    b. Choose **Reset Card** from the shortcut menu.

    c. 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 TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

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. Verify that the SBY LED is blinking on the standby card.

Step 6 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the reporting card.

Step 7 If the reseated 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 TCC+/TCC2" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

2.6.43 CTNEQPT-PBPROT

- Critical (CR), Service Affecting (SA)

The Interconnection Equipment Failure Protect Cross-Connect Card Payload Bus Alarm indicates a failure of the main payload between the Slot 10 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 TCC+/TCC2 card, or the backplane.

Note If all traffic cards show CTNEQPT-PBPROT alarm, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168 for the standby TCC+/TCC2 card. If the reseat fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-169 for the standby TCC+/TCC2 card. Do not physically reseat an active TCC+/TCC2 card. Reseating the TCC+/TCC2 disrupts traffic.

Note This alarm is automatically raised and then cleared when the Slot 8 XC card is reseated.

Caution It can take up to 30 minutes for software to be updated on a standby TCC+/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.

Procedure: Clear the CTNEQPT-PBPROT Alarm

Step 1   Perform a CTC reset on the standby cross-connect card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-169.

- While the card resets, the FAIL LED on the physical card blinks and turns off.
- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 2   Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

If the cross-connect reset is not complete and error-free or if the TCC+/TCC2 reboots automatically, call TAC (1-800-553-2447).

Step 3   If the alarm does not clear, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168 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 will be 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 2-166. 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 2-169 on the reporting card.

- While the card resets, the FAIL LED on the physical card blinks and turns off.
- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 7   Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 8   If the alarm does not clear, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168 for the reporting card.

Step 9   Complete the "Clear an External Switching Command" procedure on page 2-167.

Step 10   If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting traffic card.

⚠ **Caution**   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

Step 11   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.44 CTNEQPT-PBWORK

- Critical (CR), Service Affecting (SA)

The Interconnection Equipment Failure Working Cross-Connect Card Payload Bus alarm indicates a failure in the main payload bus between the Slot 8 cross-connect card 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 TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168 for the active TCC+/TCC2 card and then complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168. If the reseat fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-169 for the TCC+/TCC2 card. Do not physically reseat an active TCC+/TCC2 card; it disrupts traffic.

✎ **Note**   This alarm is automatically raised and then cleared when the Slot 10 XC card is reseated.

⚠ **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.

Procedure: Clear the CTNEQPT-PBWORK Alarm

Step 1   Complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-166 for the active cross-connect card.

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

Step 2   Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 for the reporting card.

- While the card resets, the FAIL LED on the physical card blinks and turns off.
- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 3   Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms window in CTC.

- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.

- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 4   If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the standby cross-connect card.

✎
Note   The ACT/STBY LED of the active card is green. The ACT/STBY 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 2-166. 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 2-169 for the reporting card.

- While the card resets, the FAIL LED on the physical card blinks and turns off.

- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 7   Verify that the reset is complete and error-free:

- No new alarms appear in the Alarms window in CTC.

- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.

- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 8   If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168 for the reporting card.

Step 9   If you switched traffic, complete the "Clear an External Switching Command" procedure on page 2-167.

Step 10   If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 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 2-169 for the reporting traffic card.

Step 12   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.45 DATAFLT

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

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

⚠

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

Procedure: Clear the DATAFLT Alarm

Step 1   Complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

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

2.6.46 DBOSYNC

- Major (MJ), Non-Service Affecting (NSA)

The standby Database Out Of Synchronization alarm occurs when the standby TCC+/TCC2 "To be Active" database does not synchronize with the active database on the active TCC+/TCC2.

⚠

Caution   If you reset the active TCC+/TCC2 card while this alarm is raised, you will lose current provisioning.

Procedure: Clear the DBOSYNC Alarm

Step 1   Save a backup copy of the active TCC+/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 if applying a provisioning change clears the alarm:

    a. In the node view, click the **Provisioning > General** tabs.

    b. In the Description field, make a small change such as adding a period to the existing entry.

    The change causes a database write but will not affect the node state. The write might take up to a minute.

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

2.6.47 DS3-MISM

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

The DS-3 Frame Format Mismatch 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 no 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.

Procedure: 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/tac for more information or call TAC (1-800-553-2447).

2.6.48 DSP-COMM-FAIL

- Major (MJ), Service Affecting (SA)

The DSP Communication Failure alarm indicates that there is a communications failure between a muxponder (MXP) or transponder (TXP) 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 or TXP card microprocessor will attempt to restore communication with the DSP chip until the alarm is cleared.

If the alarm remains for an extended period, The MXP or TXP card will raise DSP-FAIL, page 2-55.

Note   If the DSP-COMM-FAIL alarm continues for an extended period, traffic could be affected.

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

2.6.49 DSP-FAIL

- Major (MJ), Service Affecting (SA)

The DSP Failure alarm indicates that a DSP-COMM-FAIL, page 2-55, has persisted for an extended period on an MXP or TXP card. It indicates that the card is faulty.

Procedure: Clear the DSP-FAIL Alarm

Step 1   Complete the "Physically Replace a Card" procedure on page 2-169 for the reporting MXP or TXP card.

⚠️

Caution   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

2.6.50 EHIBATVG-A

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

The Extreme High Voltage Battery A alarm occurs when the voltage level on battery lead A exceeds –56.7 VDC. The alarm indicates that the voltage on the battery lead is extremely high, and power redundancy is no longer guaranteed. The alarm remains until the voltage remains under –56.7 VDC in the normal range for 120 seconds.

Procedure: Clear the EHIBATVG-A Alarm

Step 1   The problem is external to the ONS 15454. Troubleshoot the power source supplying battery lead A.

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

2.6.51 EHIBATVG-B

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

The Extreme High Voltage Battery B alarm occurs when the voltage level on battery lead B exceeds –56.7 VDC. The alarm indicates that the voltage on the battery lead is extremely high, and power redundancy is no longer guaranteed. The alarm remains until the voltage remains under –56.7 VDC in the normal range for 120 seconds.

Procedure: Clear the EHIBATVG-B Alarm

Step 1   The problem is external to the ONS 15454. Troubleshoot the power source supplying battery lead B.

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

2.6.52 ELWBATVG-A

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

The Extreme Low Voltage Battery A alarm occurs when the voltage on battery feed A is extremely low or has been lost, and power redundancy is no longer guaranteed. The extreme low voltage battery A alarm occurs when the voltage on battery feed A falls under –40.5 VDC. The alarm clears when voltage remains above –40.5 VDC in the normal range for 120 seconds.

Procedure: Clear the ELWBATVG-A Alarm

Step 1   The problem is external to the ONS 15454. Troubleshoot the power source supplying battery lead A.

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

2.6.53 ELWBATVG-B

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

The Extreme Low Voltage Battery B alarm occurs when the voltage on battery feed B is extremely low or has been lost, and power redundancy is no longer guaranteed. The extreme low voltage battery B alarm occurs when the voltage on battery feed B falls under–40.5 VDC. The alarm clears when voltage remains above –40.5 VDC in the normal range for 120 seconds.

Procedure: Clear the ELWBATVG-B Alarm

Step 1   The problem is external to the ONS 15454. Troubleshoot the power source supplying battery lead B.

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

2.6.54 EOC

- Major (MJ), Non-Service Affecting (NSA)

The SONET Data Communications Channel (DCC) Termination Failure alarm occurs when the ONS 15454 loses its data communications channel. The DCC is 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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might 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, and 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.

Procedure: Clear the EOC Alarm

Step 1 If an LOS (DS-1) alarm is also reported complete the "Clear the LOS (DS-1) Alarm" procedure on page 2-101.

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 2-165 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 OC-N 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 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 click **IS** from the pull-down menu. Click **Apply**.

Step 7 If the OC-N card is in service, use an optical test set to verify 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 might be necessary to manually switch traffic carrying circuits over to a protection path.

Step 8 If no signal failures on terminations exist, measure power levels to verify that the budget loss is within the parameters of the receiver. See the "Optical Card Transmit and Receive Levels" section on page 1-84.

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 TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

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

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

Step 11 If the TCC+/TCC2 replacement does not clear the alarm, delete the problematic DCC termination:

a. Click the **Provisioning > DCC/GCC** tabs.

b. Highlight the problematic DCC termination.

c. Click **Delete**.

d. Click **Yes** at confirmation dialog box.

Step 12 Recreate the DCC termination using the "Provision SONET DCC Terminations" procedure in the *Cisco ONS 15454 Procedure Guide*.

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 TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

2.6.55 EQPT

- Critical (CR), Service Affecting (SA)

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card.

If the EQPT alarm occurs with a BKUPMEMP alarm, see the "BKUPMEMP" section on page 2-36. 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.

Procedure: Clear the EQPT Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 for the reporting card.

- While the card resets, the FAIL LED on the physical card blinks and turns off.

- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 2 Verify that the reset is complete and error-free:

- No new alarms appear in the Alarms window in CTC.

- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.

- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 3 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 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 2-169 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.

Step 5 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.56 EQPT-MISS

- Critical (CR), Service Affecting (SA)

The Replaceable Equipment or Unit Missing alarm is reported against the fan-tray assembly unit. It indicates that the replaceable fan-tray assembly is missing or not fully inserted.

⚠
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.

Procedure: 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 2-170.

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, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.57 ERROR-CONFIG

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

The Error in Startup Configuration 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 that (1) you stored the configuration for one type of ML card in the database and then installed another type in its slot, and (2) 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*.

Procedure: Clear the ERROR-CONFIG Alarm

Step 1 If you have a different type of ML 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*.

Step 2 Upload the configuration file to the TCC+/TCC2:

   a. In the node view, right-click the ML card graphic.

   b. Choose **IOS Startup Config** from the shortcut menu.

   c. Click **Upload to TCC** and navigate to the file location.

Step 3 Complete the .

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:

   a. Right click the ML card graphic in node view.

   b. Choose **Open IOS Connection** from the shortcut menu.

> ✎
> **Note**   Open IOS Connection is not available unless the ML 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/tac for more information or call TAC (1-800-553-2447).

2.6.58 E-W-MISMATCH

- Major (MJ), Service Affecting (SA)

A Procedural Error Misconnect East/West Direction 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 might 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.

Procedure: 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 the 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 ID=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.

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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Step 10   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

Procedure: 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 Ring ID or Node ID Number" procedure on page 2-164 to identify the node ID, ring ID, 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:

   a.   Click the **Provisioning > BLSR** tabs.

   b.   Click the row from Step 3 to select it and click **Delete**.

   c.   Click **Create**.

   d.   Fill in the ring ID and node ID from the information collected in Step 3.

   e.   Click **Finish** in the BLSR Creation window.

Step 6   Display the 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.59 EXCCOL

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

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

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

Procedure: Clear the EXCCOL Alarm

Step 1   Verify that the network device port connected to the TCC+/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 TCC+/TCC2 card and the network management LAN.

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

2.6.60 EXERCISE-RING-REQ

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

The Exercise Request on Ring condition occurs when optical (traffic) cards in two-fiber and four-fiber BLSRs are tested using the EXERCISE RING command.

Note   EXERCISE-RING-REQ is an informational condition. It does not require troubleshooting.

2.6.61 EXERCISE-SPAN-REQ

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

The Exercise Request on Span condition occurs when optical (traffic) cards in a four-fiber BLSR are tested using the EXERCISE SPAN command.

Note   EXERCISE-SPAN-REQ is an informational condition. It does not require troubleshooting.

2.6.62 EXT

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

A Failure Detected External to the NE alarm occurs because an environmental alarm is present, for example, a door is open or flooding has occurred.

Procedure: Clear the EXT Alarm

Step 1   In the 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/tac for more information or call TAC (1-800-553-2447).

2.6.63 EXTRA-TRAF-PREEMPT

- Major (MJ), Service Affecting (NSA)

An Extra Traffic Preempted 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.

Procedure: 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 alarm on the working system by following the appropriate alarm in this chapter.

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

2.6.64 FAILTOSW

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

The Failure to Switch to Protection condition occurs when a working electrical (traffic) card cannot switch to the protect card in a 1:N protection group, because another working electrical (traffic) card with a higher-priority alarm has switched to the protect card.

Procedure: 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 (traffic) card that is reporting the higher priority alarm by following the "Physically Replace a Card" procedure on page 2-169. This card is the working electrical card using the 1:N card protection and not reporting FAILTOSW.

Caution   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

✎

Note   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/tac for more information or call TAC (1-800-553-2447).

2.6.65 FAILTOSW-PATH

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

The Fail to Switch to Protection Path condition occurs when the working path does not switch to the protection path on a path protection configuration. Common causes of the FAILTOSW-PATH alarm include a missing or defective protection card or a lock out set on one of the path protection configuration 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.

Procedure: Clear the FAILTOSW-PATH Condition in a Path Protection Configuration 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 2-169. 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 caries 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. Consult 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 3   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.66 FAILTOSWR

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

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

FAILTOSWR clears when one of the following actions occurs: a higher priority event, such as an external switch command occurs, the next ring switch succeeds, or the cause of the APS switch [such as an SD, page 2-139, or an SF, page 2-141] 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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Procedure: Clear the FAILTOSWR Condition in a Four-Fiber BLSR Configuration

Step 1   Perform the EXERCISE RING command on the reporting card:

   a. Click the **Provisioning > BLSR** tabs.

   b. Click the row of the affected ring under the West Switch column.

   c. Select **Exercise Ring** in the pull-down menu.

Step 2   If the condition does not clear, in the node view, click **View > 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 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 OK, 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 might 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 "Optical Card Transmit and Receive Levels" section on page 1-84 lists these specifications.

Step 11 Repeat Steps 6–10 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 2-169 for the protect standby OC-N card.

⚠ **Caution** Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

Step 13 If the condition does not clear after you replace the BLSR cards on the node one by one, follow Steps 4–12 for each of the nodes in the ring.

Step 14 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.67 FAILTOSWS

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

The Failure to Switch to Protection Span condition signals an APS span switch failure. For a four-fiber BLSR, a failed span switch initiates a ring switch. If the ring switch occurs, the FAILTOSWS condition does not appear. If the ring switch does not occur, the FAILTOSWS condition appears. FAILTOSWS clears when one of the following actions occur: 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 SD, page 2-139, or SF, page 2-141] clears.

Procedure: Clear the FAILTOSWS Condition

Step 1   Perform the EXERCISE SPAN command on the reporting card:

    a.   Click the **Maintenance > BLSR** tabs.

    b.   Determine whether the card you would like to exercise is the west card or the east card.

    c.   Click the row of the affected span under the East Switch or West Switch column.

    d.   Select **Exercise Span** in the pull-down menu.

Step 2   If the condition does not clear, in the node view, click **View > 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 OK, 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 might 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 "Optical Card Transmit and Receive Levels" section on page 1-84 lists these specifications.

Step 11   Repeat Steps 6–10 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 2-169 for the protect standby OC-N card.

⚠

Caution   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

Step 13   If the condition does not clear after you replace the BLSR cards on the node one by one, follow Steps 4–12 for each of the nodes in the ring.

Step 14   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.68 FAN

- Critical (CR), Service Affecting (SA)

The Fan Failure alarm indicates a problem with the fan-tray assembly. When the fan-tray assembly is not fully functional, the temperature of the ONS 15454 can rise above its normal operating range. The fan-tray assembly contains six fans and needs a minimum of five working fans to properly cool the ONS 15454. However, even with five working fans, the fan-tray assembly can 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.

Procedure: Clear the FAN Alarm

Step 1   Verify 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 2-170.

✎

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 3-11.

Step 4   If the replacement fan-tray assembly does not operate correctly, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.69 FANDEGRADE

- Major (MJ), Non-Service Affecting (NSA)

The Partial Fan Failure Speed Control Degradation 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.

Procedure: Clear the FANDEGRADE Alarm

Step 1   Complete the "Clear the FAN Alarm" procedure on page 2-70.

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

2.6.70 FE-AIS

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

The Far-End AIS condition occurs when an AIS has occurred at the far-end node. FE-AIS usually occurs in conjunction with an LOS (OC-N), page 2-105, downstream.

Procedure: Clear the FE-AIS Condition

Step 1   Complete the "Clear the AIS Condition" procedure on page 2-21.

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

2.6.71 FE-DS1-MULTLOS

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

The Far-End Multiple DS-1 LOS Detected 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. Both alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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/tac for more information or call TAC (1-800-553-2447).

2.6.72 FE-DS1-NSA

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

The Far End DS-1 Equipment Failure Non-Service Affecting 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. Both the alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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/tac for more information or call TAC (1-800-553-2447).

2.6.73 FE-DS1-SA

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

The Far End DS-1 Equipment Failure Service Affecting 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. Both the alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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/tac for more information or call TAC (1-800-553-2447).

2.6.74 FE-DS1-SNGLLOS

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

The Far-End Single DS-1 LOS condition occurs when a single DS-1 signal is lost on far-end DS-1 equipment. Signal loss also causes an LOS (OC-N), page 2-105. 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. Both alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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/tac for more information or call TAC (1-800-553-2447).

2.6.75 FE-DS3-NSA

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

The Far End DS-3 Equipment Failure Non-Service Affecting 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. Both the alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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/tac for more information or call TAC (1-800-553-2447).

2.6.76 FE-DS3-SA

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

The Far End DS-3 Equipment Failure Service Affecting 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. Both alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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/tac for more information or call TAC (1-800-553-2447).

2.6.77 FE-EQPT-NSA

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

The Far End Common Equipment Failure 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. Both 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.

Procedure: 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 might 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/tac for more information or call TAC (1-800-553-2447).

2.6.78 FE-EXERCISING-RING

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

The Far End Exercising Ring condition occurs when far-end optical (traffic) cards in a two-fiber or four-fiber BLSR are being tested using the EXERCISE RING command.The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-EXERCISING-RING condition.

Note   FE-EXERCISING-RING is an informational condition. It does not require troubleshooting.

2.6.79 FE-EXERCISING-SPAN

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

The Far End Exercising Span condition occurs when far-end optical (traffic) cards in a four-fiber BLSR are being tested using the EXERCISE SPAN command.The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-EXERCISING-SPAN condition.

Note   FE-EXERCISING-SPAN is an informational condition. It does not require troubleshooting.

2.6.80 FE-FRCDWKSWPR-RING

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

The Far End Ring Working Facility Forced to Switch to Protection 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. Both the alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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 Span Lock Out" procedure on page 2-165 for instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.81 FE-FRCDWKSWPR-SPAN

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

The Far End Working Facility Forced to Switch to Protection 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. Both the alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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 Span Lock Out" procedure on page 2-165 for instructions.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.82 FE-IDLE

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

The Far End 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.

Procedure: 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 might 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 Span Lock Out" procedure on page 2-165.

Step 4   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.83 FE-LOCKOUTOFPR-SPAN

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

The Far-End lock out of Protection Span condition occurs when a BSLR span is locked out of the protection system from a far-end node using the LOCKOUT 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. Both the alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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   Make sure there is no lock out set. See the "Clear a BLSR Span Lock Out" procedure on page 2-165 for instructions.

Step 4   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.84 FE-LOF

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

The Far End LOF condition occurs when a far-end node reports an LOF (DS-3), page 2-95.

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. Both alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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 (DS-1) Alarm" procedure on page 2-94. It also applies to FE-LOF.

Step 4   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.85 FE-LOS

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

The Far End LOS condition occurs when a far-end node reports an LOS (DS-3), page 2-102.

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. Both alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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 (DS-1) Alarm" procedure on page 2-101.

Step 4   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.86 FE-MANWKSWPR-RING

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

The Far End Ring Manual Switch of Working Facility to Protect condition occurs when a BLSR working ring is switched from working to protect at a 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. Both the alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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 Span Lock Out" procedure on page 2-165.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.87 FE-MANWKSWPR-SPAN

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

The Far-End Manual Switch Span Working Facility to Protect 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. Both the alarms or conditions clear when the main alarm clears.

Procedure: 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 might 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 Span Lock Out" procedure on page 2-165.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.88 FEPRLF

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

The Far End Protection Line Failure alarm occurs when an APS channel SF, page 2-141, 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 4-fiber BLSR configuration.

Procedure: 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 might relate to a main alarm from a card in Slot 6 of Node 2.

Step 2   Log into the node that links directly to the card reporting the FE condition.

Step 3   Clear the main alarm. Refer to the appropriate alarm section in this chapter in this chapter for instructions.

Step 4   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.89 FORCED-REQ

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

The Force Switch Request on Facility or Equipment 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.

Procedure: Clear the FORCED-REQ Condition

Step 1   Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165.

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

2.6.90 FORCED-REQ-RING

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

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

Procedure: Clear the FORCED-REQ-RING Condition

Step 1   Complete the "Clear the FORCED-REQ Condition" procedure on page 2-80.

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

2.6.91 FORCED-REQ-SPAN

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

The Force Switch Request 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.

Procedure: Clear the FORCED-REQ-SPAN Condition

Step 1   Complete the "Clear the FORCED-REQ Condition" procedure on page 2-80.

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

2.6.92 FRCDSWTOINT

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

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

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

2.6.93 FRCDSWTOPRI

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

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

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

2.6.94 FRCDSWTOSEC

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

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

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

2.6.95 FRCDSWTOTHIRD

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

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

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

2.6.96 FRNGSYNC

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

The Free Running Synchronization Mode 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 BITS timing source. After the 24-hour holdover period expires, timing slips might begin to occur on an ONS 15454 relying on an internal clock.

Procedure: Clear the FRNGSYNC Alarm

Step 1   If the ONS 15454 is configured to operate from its internal clock, disregard the FRNGSYNC alarm.

Step 2   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.

Step 3   If the BITS source is valid, clear alarms related to the failures of the primary and secondary reference sources, such as SYNCPRI, page 2-153, and SYNCSEC, page 2-154.

Step 4   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.97 FSTSYNC

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

A Fast Start Synchronization mode 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/tac for more information or call TAC (1-800-553-2447).

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

2.6.98 FULLPASSTHR-BI

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

The Bidirectional Full Pass-Through Active condition occurs on a non-switching 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.

Procedure: Clear the FULLPASSTHR-BI Condition

Step 1   Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165.

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

2.6.99 GCC-EOC

- Major (MJ), Non-Service Affecting (NSA)

The GCC Embedded Operation Channel Failure alarm applies to the OTN communication channel for TXP and MXP cards. The GCC-EOC is raised when the channel cannot operate.

Procedure: Clear the GCC-EOC Alarm

Step 1   Complete the "Clear the EOC Alarm" procedure on page 2-58.

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

2.6.100 HI-LASERBIAS

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

The Equipment High Transmit Laser Bias Current alarm is raised against the TXP and MXP card laser performance. The alarm indicates that the card laser has reached the maximum laser bias tolerance.

Laser bias typically starts at about 30% of the manufacturer's maximum laser bias specification and increases as the laser ages. So if the HI-LASERBIAS alarm threshold is set at 100% of the maximum, the laser's usability has ended. If the threshold is set at 90% of the maximum, the card is still usable for several weeks or months before it needs to be replaced.

Procedure: Clear the HI-LASERBIAS Alarm

Step 1   Complete the "Clear the LASEREOL Alarm" procedure on page 2-91. Replacement is not urgent and can be scheduled during a maintenance window.

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

2.6.101 HI-LASERTEMP

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

The Equipment High Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. HI-LASERTEMP occurs when the internally measured transceiver temperature exceeds the card default level by 2° C.

✎
Note To verify the card laser temperature level, double-click the card in node view and click the **Performance > Optics PM** tabs. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Procedure: Clear the HI-LASERTEMP Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 for the reporting MXP or TXP card.

Step 2 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting MXP or TXP card.

⚠
Caution Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC at 1-800-553-2447.

2.6.102 HI-RXPOWER

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

The Equipment High Receive Power alarm is an indicator of the optical signal power that is transmitted to the TXP or MXP card. HI-RXPOWER occurs when the measured optical power of the received signal exceeds the threshold. The threshold value is user-provisionable.

Procedure: Clear the HI-RXPOWER Alarm

Step 1 Find out whether gain (the amplification power) of any amplifiers has been changed. The change will also cause 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 off, the power levels of all channels will have to be adjusted.

✎
Note If the card is part of an amplified dense wavelength 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 will be garbled and receive power will increase by about +3dB.

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 known-good loopback cable to complete the "Perform a Facility Loopback on a Source DS-N Port" procedure on page 1-5.

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 2-169. 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 caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

Step 8   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.103 HI-RXTEMP

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

The Equipment High Receive temperature alarm refers to the temperature of the trunk card port for the TXP and MXP cards. The HI-RXTEMP threshold is user-provisionable.

Procedure: Clear the HI-RXTEMP Alarm

Step 1   If an EXT alarm is also present, complete the "Clear the EXT Alarm" procedure on page 2-64.

Step 2   If a shelf HITEMP alarm is also present, complete the "Clear the HITEMP Alarm" procedure on page 2-86.

Step 3   If a HI-LASERTEMP alarm is also present, complete the "Clear the HI-LASERTEMP Alarm" procedure on page 2-84.

✎

Note   If no data alarms have occurred, the card does not need to be replaced immediately.

Step 4   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.104 HITEMP

- Critical (CR), Service Affecting (SA) for NE

- Minor (MN), Non-Service Affecting (NSA) for EQPT

The High Temperature alarm occurs when the temperature of the ONS 15454 is above 122° F (50° 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.

Procedure: Clear the HITEMP Alarm

Step 1   View the temperature displayed on the ONS 15454 LCD front panel. For an illustration of the LCD panel, refer to NTP-70, "View Alarm Counts on the LCD for a Slot or Port," in the *Cisco ONS 15454 Procedure Guide*.

Step 2   Verify whether 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, verify whether the air filter to see whether it needs replacement. Refer to NTP-107, "Inspect and Maintain the Air Filter," in the *Cisco ONS 15454 Procedure Guide*

Step 6   If the filter is clean, complete the "Remove and Reinsert Fan-Tray Assembly" procedure on page 2-170.

✏️

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 3-11.

Step 8   If the replacement fan-tray assembly does not operate correctly, log onto http://www.cisco.com/tac for more information or call 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.

2.6.105 HI-TXPOWER

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

The Equipment High Transmit Power alarm is an indicator on the TXP card and MXP card transmitted optical signal power. HI-TXPOWER occurs when the measured optical power of the transmitted signal exceeds the threshold.

Procedure: Clear the HI-TXPOWER Alarm

Step 1   In the node view, display the card view for the TXP or MXP card.

Step 2   Click the **Provisioning > Optical Thresholds** tabs.

Step 3   Decrease (i.e. 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 2-169.

⚠️

Caution   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

Step 5   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.106 HLDOVRSYNC

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

The Holdover Synchronization Mode 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.

Procedure: Clear the HLDOVRSYNC Alarm

Step 1   Clear additional alarms that relate to timing, such as FRNGSYNC, page 2-82; FSTSYNC, page 2-82; HLDOVRSYNC, page 2-87; LOS (BITS), page 2-101; LOS (BITS), page 2-101; MANSWTOINT, page 2-112; MANSWTOPRI, page 2-112; MANSWTOSEC, page 2-113; MANSWTOTHIRD, page 2-113; SWTOPRI, page 2-152; SWTOSEC, page 2-152; SWTOTHIRD, page 2-152; SYNC-FREQ, page 2-153; SYNCPRI, page 2-153; SYNCSEC, page 2-154, or SYNCTHIRD, page 2-154.

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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.107 IMPROPRMVL

- Critical (CR), Service Affecting (SA)

The Improper Removal 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   It can take up to 30 minutes for software to be updated on a standby TCC+/TCC2 card.

⚠

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.

Procedure: Clear the IMPROPRMVL Alarm

Step 1   In the 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, take them out of service (OOS):

⚠

Caution   Before taking 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** 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 .

⚠

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 the 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** 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.108 INC-ISD

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

The DS-3 Idle condition indicates that the DS-3 card is receiving an idle signal, meaning that the payload of the signal contains a repeating pattern of bits. The INC-ISD condition occurs when the transmitting port has an 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.

2.6.109 INHSWPR

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

The Inhibit Switch To Protect Request on Equipment condition occurs on traffic cards when the ability to switch to protect has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the working system. If the card is part of a1:N protection scheme, traffic can be switched between working cards when the switched to protect is disabled.

Procedure: Clear the INHSWPR Condition

Step 1   Complete the "Clear an External Switching Command" procedure on page 2-167.

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

2.6.110 INHSWWKG

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

The Inhibit Switch To Working Request on Equipment condition occurs on traffic cards when the ability to switch to working has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the protect system. If the card is part of a1:N protection scheme, traffic can be switched between protect cards when the switched to working is disabled.

Procedure: Clear the INHSWWKG Condition

Step 1 Complete the "Clear an External Switching Command" procedure on page 2-167.

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

2.6.111 INVMACADR

- Major (MJ), Non-Service Affecting (NSA)

The Equipment Failure Invalid MAC Address alarm occurs when the ONS 15454 Media Access Control layer address (MAC Address) is invalid. The MAC Address is permanently assigned to the ONS 15454 chassis when it is manufactured. Do not attempt to troubleshoot an INVMACADR. Contact TAC at 1-800-553-2447.

2.6.112 KB-PASSTHR

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

The K Bytes Pass Through Active condition occurs on a non-switching node in a BLSR when the protect channels on the node are not active and the node is in K Byte Pass-Through State.

Procedure: Clear the KB-PASSTHR Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165.

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

2.6.113 LAN-POL-REV

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

The Lan Connection Polarity Reversed condition is raised by the TCC+ card 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. This condition usually occurs during software upgrades to Release 4.0 or in new NE installations.

⚠ **Caution**   If you upgrading from a TCC-I card to a TCC2 card, you must resolve this condition before you begin the upgrade. The TCC2 card does not compensate for reversed polarity.

Procedure: 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 condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.114 LASEREOL

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

The Laser Approaching End of Life alarm applies to TXP and MXP cards. It is typically accompanied by HI-LASERBIAS, page 2-83. 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%, the laser replacement can usually be done during a maintenance window. But if the HI-LASERBIAS threshold is set at 100% and is accompanied by data errors, the card must be replaced sooner.

Procedure: Clear the LASEREOL Alarm

Step 1   Complete the "Physically Replace a Card" procedure on page 2-169.

⚠ **Caution**   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

2.6.115 LKOUTPR-S

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

The Lockout of Protection Span condition occurs on a BSLR node when traffic is locked out of a protect span using the LOCKOUT SPAN command.

Procedure: Clear the LKOUTPR-S Condition

Step 1   Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165.

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

2.6.116 LMP-HELLODOWN

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

The Link Management Protocol (LMP) Hello Down alarm 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.

Procedure: 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 there is no LOF (OC-N) alarm on the source or destination nodes. If there is complete the "Clear the LOS (DS-3) Alarm" procedure on page 2-103.

Step 3   If the alarm does not clear, complete the "Clear the CKTDOWN Alarm" procedure on page 2-43 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/tac for more information or call TAC (1-800-553-2447).

2.6.117 LMP-NDFAIL

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

The LMP Neighbor Detection Fail 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.

Procedure: Clear the LMP-NDFAIL Alarm

Step 1   Complete the "Clear the LMP-HELLODOWN Alarm" procedure on page 2-92.

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

2.6.118 LOCKOUT-REQ

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

The Lockout Switch Request on Facility/Equipment condition occurs when a user initiates a lock out switch request for an OC-N card or a lock out switch request on a path protection configuration at the path level. A lock out prevents protection switching. Clearing the lock out again allows protection switching and clears the LOCKOUT-REQ condition.

Procedure: Clear the LOCKOUT-REQ Condition

Step 1   Complete the "Clear a Path Protection Lock Out" procedure on page 2-166.

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

2.6.119 LOCKOUT-REQ-RING

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

The Lockout Switch Request Ring condition occurs when a LOCKOUT RING command is applied to a BLSR to prevent all protection switching on the ring.

Procedure: Clear the LOCKOUT-REQ-RING Condition

Step 1   Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165.

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

2.6.120 LOF (BITS)

- Major (MJ), Service Affecting (SA)

The Loss of Frame (LOF) BITS alarm occurs when a port on the TCC+/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 turnup.

Cisco ONS 15454 Troubleshooting Guide, R4.0

Procedure: Clear the LOF (BITS) Alarm

Step 1   Verify that the line framing and line coding match between the BITS input and the TCC+/TCC2:

    a.   In node view or card view, note the slot and port reporting the alarm.

    b.   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.

    c.   Click the **Provisioning > Timing** tabs to display the General Timing window.

    d.   Verify that Coding matches the coding of the BITS timing source, either B8ZS or AMI.

    e.   If the coding does not match, click **Coding** and choose the appropriate coding from the pull-down menu.

    f.   Verify that Framing matches the framing of the BITS timing source, either ESF or SF (D4).

    g.   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 TCC+/TCC2, complete the "Physically Replace a Card" procedure on page 2-169 for the TCC+/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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.121 LOF (DS-1)

- Major (MJ), Service Affecting (SA)

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 might have its framing set to a format that differs from the receiving ONS 15454.

Procedure: Clear the LOF (DS-1) 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 might 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.122 LOF (DS-3)

- Critical (CR), Service Affecting (SA)

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 might 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.

Procedure: Clear the LOF (DS-3) 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.123 LOF (EC-N)

- Critical (CR), Service Affecting (SA)

The EC-N LOF alarm occurs when a port on the reporting OC-N 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.

Procedure: Clear the LOF (EC-N) Alarm

Step 1   Verify cabling continuity to the port reporting the alarm.

Step 2   If cabling continuity is OK, 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 TAC to report a service-affecting problem (1-800-553-2447).

2.6.124 LOF (OC-N)

- Critical (CR), Service Affecting (SA)

The LOF alarm occurs when a port on the reporting OC-N 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.

Procedure: Clear the LOF (OC-N) Alarm

Step 1   Verify cabling continuity to the port reporting the alarm.

Step 2   If cabling continuity is OK, 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 TAC to report a service-affecting problem (1-800-553-2447).

2.6.125 LO-LASERBIAS

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

The Equipment Low Transmit Laser Bias Current alarm is raised against the TXP and MXP card laser performance. The alarm indicates that the card laser has reached the minimum laser bias tolerance.

If the LO-LASERBIAS alarm threshold is set at 0% (the default), the laser's usability has ended. If the threshold is set at 5% to10%, the card is still usable for several weeks or months before you need to replace it.

Procedure: Clear the LO-LASERBIAS Alarm

Step 1   Complete the "Clear the LASEREOL Alarm" procedure on page 2-91.

Replacement is not urgent and can be scheduled during a maintenance window.

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

2.6.126 LO-LASERTEMP

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

The Equipment Low Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. LO-LASERTEMP occurs when the internally measured transceiver temperature falls 2° C under the card default level.

Note   To verify the card laser temperature level, double-click the card in node view and click the **Performance > Optics PM** tabs. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Procedure: Clear the LO-LASERTEMP Alarm

Step 1   Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 for the reporting MXP or TXP card.

Step 2   If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting MXP or TXP card.

⚠
Caution   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

2.6.127 LOM

- Critical (CR), Service Affecting (SA)

The Loss of Multiframe alarm applies to MXP and TXP cards when the MFAS overhead field is errored for more than five frames and persists for more than three milliseconds.

Procedure: Clear the LOM Alarm

Step 1   Complete the "Clear the SD Condition" procedure on page 2-140.

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

2.6.128 LOP-P

- Critical (CR), Service Affecting (SA)

A Loss of Pointer Path alarm indicates that the SONET path pointer in the overhead has been lost. LOP occurs when valid H1/H2 pointer bytes are missing from the overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SONET payload. An LOP-P alarm occurs when eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

The LOP-P alarm can occur when the received payload does not match the provisioned payload. The alarm is caused by a circuit type mismatch on the concatenation facility. For example, if an STS-1 is sent across a circuit provisioned for STS-3c, an LOP-P alarm occurs.

⚠
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.

Procedure: Clear the LOP-P Alarm

Step 1   In the 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 2-167.

Step 5   Recreate the circuit for the correct size. For instructions, see the "Create Circuits and VT Tunnels" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 6   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.129 LOP-V

- Major (MJ), Service Affecting (SA)

The LOP VT alarm indicates a loss of pointer at the VT level.

The LOP-V alarm can occur when the received payload does not match the provisioned payload. LOP-V is caused by a circuit size mismatch on the concatenation facility.

⚠️
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.

Procedure: Clear the LOP-V Alarm

Step 1   Complete the "Clear the LOP-P Alarm" procedure on page 2-98.

Step 2   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.130 LO-RXPOWER

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

The Equipment Low Receive Power alarm is an indicator for TXP card and MXP 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.

Procedure: 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 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 will also cause 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 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 Loopback on a Source DS-N Port" procedure on page 1-5.

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 2-169. 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 caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

Step 9   If no ports are shown bad and the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.131 LO-RXTEMP

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

The Equipment Low Receive temperature alarm refers to the temperature of the trunk card port for the TXP and MXP cards. The LO-RXTEMP threshold is user-provisionable. The alarm does not occur unless the RxTemp Low threshold is set above 0° F or C.

Procedure: Clear the LO-RXTEMP Alarm

Step 1   If this alarm accompanies other receive or transmit alarms for power, troubleshoot these alarms first.

Step 2   If the alarm does not clear, display the MXP or TXP card view.

Step 3   Click the **Provisioning > Optical Thresholds** tabs.

Step 4   Adjust the temperature in the Rx Temp Low column down a few degrees.

Step 5   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.132 LOS (BITS)

- Major (MJ), Service Affecting

The LOS (BITS) alarm indicates that the TCC+/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.

Procedure: 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 OK, verify that the BITS clock is operating properly.

Step 3   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.133 LOS (DS-1)

- Major (MJ), Service Affecting (SA)

A LOS (DS-1) alarm for a DS-3 port or 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. 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.

Procedure: Clear the LOS (DS-1) Alarm

Step 1   Verify cabling continuity to the port.

Step 2   If the cabling is OK, 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 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 DS-N connector on the ONS 15454.

Step 6   Repeat Steps 1–5 for any other port on the card that reports the LOS (DS-1).

Step 7   If the alarm does not clear, look for and troubleshoot any other alarm that might identify the source of the problem.

Step 8   If no other alarms are present that might 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 2-169 for the reporting card.

⚠ **Caution**   Removing a card that currently caries 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. Consult 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 9   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.134 LOS (DS-3)

- Critical (CR), Service Affecting (SA)

The LOS (DS-3) for either a DS-3 port or 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. 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 and will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Procedure: Clear the LOS (DS-3) Alarm

Step 1   Verify cabling continuity to the port.

Step 2   If the cabling is OK, 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 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 DS-N connector on the ONS 15454.

Step 6   Repeat Steps 1–5 for any other port on the card that reports the LOS (DS-3).

Step 7   If the alarm does not clear, look for and troubleshoot any other alarm that might identify the source of the problem.

Step 8   If no other alarms exist that might be the source of the LOS (DS-3), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting card.

⚠

Caution   Removing a card that currently caries 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. Consult 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 9   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.135 LOS (EC-N)

- Critical (CR), Service Affecting (SA)

LOS on an EC-N port occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS (EC-N) means the upstream transmitter has failed. If an EC-N LOS alarm is not accompanied by additional alarms, a fiber break or 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 and will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Procedure: Clear the LOS (EC-N) Alarm

Step 1   Verify cabling continuity to the port reporting the alarm.

Step 2   If the cabling is OK, 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 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 1–5 for any other port on the card that reports the LOS (EC-N).

Step 7   If the alarm does not clear, look for and troubleshoot any other alarm that might identify the source of the problem.

Step 8   If no other alarms exist that might be the source of the LOS (EC-N), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting card.

⚠

Caution   Removing a card that currently caries 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. Consult 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 9   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.136 LOS (OC-N)

- Critical (CR), Service Affecting (SA)

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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might 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 and will be able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Procedure: Clear the LOS (OC-N) Alarm

Step 1   Verify fiber continuity to the port.

Step 2   If the cabling is OK, 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 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 "Optical Card Transmit and Receive Levels" section on page 1-84 lists these specifications for each card.

Step 5   If 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 1–6 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 might identify the source of the problem.

Step 9   If no other alarms exist that might 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 2-169 for the reporting card.

⚠

Caution   Removing a card that currently caries 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. Consult 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 10   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.137 LO-TXPOWER

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

The Equipment Low Transmit Power alarm is an indicator for TXP card and MXP 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.

Procedure: Clear the LO-TXPOWER Alarm

Step 1   Display the MXP or TXP 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 2-169.

⚠

Caution   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

Step 5   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.138 LPBKCRS

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

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

For more information on loopbacks, see the "Identify Points of Failure on a DS-N Circuit Path" section on page 1-5.

Clear the LBKCRS 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   Under 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/tac for more information or call TAC (TAC) at 1-800-553-2447.

2.6.139 LPBKDS1FEAC

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

A Loopback Caused by FEAC Command DS-1 condition on the DS3XM-6 card occurs when a DS-1 loopback signal is received from the far-end node due to a Far-End Alarm and Control (FEAC) command. An FEAC command is often used with loopbacks.

Procedure: Clear the LPBKDS1FEAC Condition

Step 1   At the node view, double-click the DS3XM-6 card to display the card view.

Step 2   Click the **Maintenance > DS1** tabs.

Step 3   Click the Send Code column, cell for the port and click **No Code** from the pull-down menu.

Step 4   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (TAC) at 1-800-553-2447.

2.6.140 LPBKDS1FEAC-CMD

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

The DS-1 Loopback Command Sent To Far End 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 1-22.

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

2.6.141 LPBKDS3FEAC

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

A Loopback Due to FEAC Command DS-3 condition occurs when a DS3XM-6 card loopback signal is received from the far-end node because of a Far-End Alarm and Control (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.

Procedure: Clear the LPBKDS3FEAC Condition

Step 1   At the node view, double-click the DS3XM-6 card to display the card view.

Step 2   Click the **Maintenance > DS3** tabs.

Step 3   Click the Send Code column, cell for the port and click **No Code** from the pull-down menu.

Step 4   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (TAC) at 1-800-553-2447.

2.6.142 LPBKDS3FEAC-CMD

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

The DS-3 Loopback Command Sent To Far End 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 1-22.

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

2.6.143 LPBKFACILITY (DS-1 or DS-3)

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

A Loopback Facility condition occurs when a software facility loopback is active for a port on the reporting card.

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 1-5.

Caution   CTC permits you to perform loopbacks on an in-service (IS) circuit, but 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 LPBKFACILITY condition can also be accompanied by a more serious alarm such as LOS.

Note   DS3XM-6 cards only support facility loopbacks on DS-1 circuits.

Procedure: Clear the LPBKFACILITY (DS-1 or DS-3) Condition

Step 1   From the 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 Loopback" procedure on page 2-167.

Step 4   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.144 LPBKFACILITY (EC-N)

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

A Loopback Facility condition occurs when a software facility loopback is active for a port on the reporting card.

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 1-5.

⚠️

Caution   CTC permits you to perform loopbacks on an in-service (IS) circuit, but 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 LPBKFACILITY condition can also be accompanied by a more serious alarm such as LOS..

Procedure: Clear the LPBKFACILITY (EC-N) Condition

Step 1   The loopback originates from the DS3XM-6 card. Complete the "Clear the LPBKDS3FEAC Condition" procedure on page 2-108.

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

2.6.145 LPBKFACILITY (OC-N)

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

A Loopback Facility condition occurs when a software facility loopback is active for a port on the reporting card.

For more information about loopbacks, see the "Identify Points of Failure on an OC-N Circuit Path" section on page 1-23.

⚠️

Caution   CTC permits you to perform loopbacks on an in-service (IS) circuit, but 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 LPBKFACILITY condition can also be accompanied by a more serious alarm such as LOS.

Procedure: Clear the LPBKFACILITY (OC-N) Condition

Step 1   Complete the "Clear a Loopback" procedure on page 2-167.

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

⚠️

Caution   Before performing a facility loopback on an OC-N card, make sure the card contains at least two DCC paths to the node where the card is installed. A second DCC path provides a non-looped 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.

2.6.146 LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N)

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

A Loopback Terminal condition occurs when a software terminal loopback is active for a port on the reporting card.

> **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.

Procedure: Clear the LPBKTERMINAL (DS-1, DS-3, EC-1-12, OC-N) Condition

Step 1 Complete the "Clear a Loopback" procedure on page 2-167.

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

> **Note** Terminal loopback is not supported at the DS-1 level for the DS3XM-6 card.

2.6.147 LPBKTERMINAL (G-Series)

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

A Loopback Terminal condition occurs when a software terminal loopback is active for a port on the reporting card.

When a port in terminal 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. G1000-4 cards only support terminal loopbacks.

> **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.

Procedure: Clear the LPBKTERMINAL (G-Series) Condition

Step 1 Complete the "Clear a Loopback" procedure on page 2-167.

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

2.6.148 MAN-REQ

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

The Manual Switch Request on a Facility/Equipment condition occurs when a user initiates a manual switch request on an OC-N card or path protection configuration path. Clearing the manual switch clears the MAN-REQ condition.

Procedure: Clear the MAN-REQ Condition

Step 1   Complete the "Clear a Path Protection Lock Out" procedure on page 2-166.

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

2.6.149 MANRESET

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

A User-Initiated Manual Reset condition occurs when you right-click a card in CTC and choose Reset. Resets performed during a software upgrade also prompt the condition. The MANRESET condition clears automatically when the card finishes resetting.

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

2.6.150 MANSWTOINT

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

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

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

2.6.151 MANSWTOPRI

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

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

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

2.6.152 MANSWTOSEC

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

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

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

2.6.153 MANSWTOTHIRD

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

The Manual Switch To Third Reference 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.

2.6.154 MANUAL-REQ-RING

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

The Manual Switch Request on Ring condition occurs when a user initiates a MANUAL RING command on two-fiber and four-fiber BLSR rings to switch from working to protect or protect to working.

Procedure: Clear the MANUAL-REQ-RING Condition

Step 1   Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165.

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

2.6.155 MANUAL-REQ-SPAN

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

The Manual Switch Request on Ring 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.

Procedure: Clear the MANUAL-REQ-SPAN Condition

Step 1   Complete the "Clear a BLSR Span Lock Out" procedure on page 2-165.

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

2.6.156 MEA (AIP)

- Critical (CR), Service Affecting (SA)

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-Amp fuse is installed in a newer 10 Gbps-compatible or ANSI shelf assembly (15454-SA-ANSI).

Procedure: 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.157 MEA (BP)

- Critical (CR), Service Affecting (SA)

The MEA alarm for the backplane occurs when the revision of the backplane is incompatible with cross-connect equipment.

Procedure: Clear the MEA (BP) Alarm

Step 1   If the MEA is also raised against other equipment, such as the AIP or a fan-tray assembly, troubleshoot these alarms first.

Step 2   If alarms are reported directly against the cross-connect card, such as SWMTXMOD, page 2-150, troubleshoot these alarms next.

Step 3   If the alarm does not clear, determine whether the ONS 15454 shelf assembly is a newer ANSI 10-Gbps compatible shelf assembly (15454-SA-ANSI) or an earlier shelf assembly:

   a.   At the node view, click the **Inventory** tab.

   b.   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 or 10-Gbps compatible shelf assembly.

   c.   Under the **HW Part #** column, if the number is not 800-19856-XX or 800-19856-XX, then you are using an earlier shelf assembly.

   ✎
   Note   On the 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 4   If the shelf assembly is not compatible with 10-Gbps equipment, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.158 MEA (EQPT)

- Critical (CR), Service Affecting (SA)

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, pre-ANSI shelf assembly or when older Ethernet (traffic) cards (E1000-2 and E100T-12) are used in a newer ANSI 10-Gbps compatible shelf assembly. Removing the incompatible cards clears the alarm.

Note   If an OC3-8 card is installed in a high-speed slot (Slots 5-6 and 12-13), it will not appear in CTC and will raise an MEA.

Procedure: Clear the MEA (EQPT) Alarm

Step 1   Determine whether the ONS 15454 shelf assembly is a newer ANSI 10-Gbps compatible shelf assembly (15454-SA-ANSI) or an earlier shelf assembly. In the node view, click the **Inventory** tab.

Under the **HW Part #** column, if the part number is 800-19857-XX, then you have a 15454-SA-ANSI shelf or 10-Gbps compatible shelf assembly.

Under the **HW Part #** column, if the number is not 800-19856-XX, then you are using an earlier shelf assembly.

Note   On the 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 ANSI 10-Gbps compatible shelf assembly (15454-SA-ANSI) and the card reporting the alarm is not an E1000-2 or E100T-12, proceed to Step 3.

b.   If you have a newer ANSI 10-Gbps compatible shelf assembly (15454-SA-ANSI) 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, non-compatible 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 ANSI 10-Gbps compatible shelf assembly.

    c. If you have a pre-ANSI 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 a pre-ANSI 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 2-169 for the reporting card.

> ⚠
> **Caution** Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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, take them out of service (OOS):

> ⚠
> **Caution** Before taking ports out of service, ensure that no live traffic.

    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 2-167.

> ⚠
> **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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.159 MEA (FAN)

- Critical (CR), Service Affecting (SA)

The MEA alarm is reported against the fan-tray assembly when a newer fan-tray assembly (15454-FTA3) with a 5 Amp fuse is used with an older shelf assembly or when an older fan-tray assembly with a 2-Amp fuse is used with a newer 10-Gbps compatible or ANSI shelf assembly (15454-SA-ANSI) that contains cards introduced in Release 3.1 or later. If a newer ANSI 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.

Procedure: Clear the MEA (FAN) Alarm

Step 1 Determine whether the ONS 15454 shelf assembly is a newer ANSI 10-Gbps compatible shelf assembly (15454-SA-ANSI) 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 or 10-Gbps compatible shelf assembly.

Under the **HW Part #** column, if the number is not 800-19857-XX or 800-19856-XX, then you are using an earlier shelf assembly.

Step 2 If you have a 15454-SA-ANSI shelf or 10-Gbps compatible shelf assembly, 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 Amp fuse and complete the "Replace the Fan-Tray Assembly" procedure on page 3-11.

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 3-11.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.160 MEM-GONE

- Major (MJ), Non-Service Affecting (NSA)

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TCC+/TCC2 card. CTC does not function properly until the alarm clears. The alarm clears when additional memory becomes available.

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

2.6.161 MEM-LOW

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

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

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

2.6.162 MFGMEM

- Critical (CR), Service Affecting (SA)

The MFGMEM or Manufacturing Data Memory Failure alarm occurs if the ONS 15454 cannot access the data in the erasable programmable read-only memory (EEPROM). Either the memory module on the component failed or the TCC+/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.

Procedure: Clear the MFGMEM (AIP, BP, Fan-Tray Assembly) Alarm

Step 1   Complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

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 TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

Step 3   If the MFGMEM alarm continues to report after replacing the TCC+/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 3-11.

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/tac for more information or call TAC (1-800-553-2447).

Step 6   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.163 NO-CONFIG

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

The No Startup Configuration alarm applies to ML-series Ethernet (traffic) cards and occurs when you pre-provision a high-speed slot (Slots 5-6 and 12-13) for the card without inserting the card first, or when you insert a card without pre-provisioning. (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 TCC+/TCC2, the alarm clears.

Procedure: Clear the NO-CONFIG Alarm

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 TCC+/TCC2:

   a.   In the node view, right-click the ML card graphic.

   b.   Choose **IOS Startup Config** from the shortcut menu.

   c.   Click **Upload to TCC** and navigate to the file location.

Step 3   Complete the "Reset a Traffic Card in CTC" procedure on page 2-169.

Step 4   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.164 NOT-AUTHENTICATED

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

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.

Note   NOT-AUTHENTICATED is an informational alarm and is resolved when CTC successfully logs into the node.

2.6.165 ODUK-AIS-PM

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

The Optical Data Unit (ODUK) AIS Path Monitoring (PM) condition applies to TXP cards and MXP cards when G.709 monitoring is enabled for the cards. It is a secondary condition that indicates a more serious condition such as LOS (OC-N), page 2-105, is 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 an ODUK-OCI-PM, page 2-121, upstream.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: Clear the ODUK-AIS-PM Condition

Step 1   Verify whether upstream nodes and equipment have alarms, especially an LOS (OC-N), page 2-105, or OOS ports.

Step 2   Clear the upstream alarms using the applicable procedure(s) in this chapter.

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

2.6.166 ODUK-BDI-PM

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

The ODUK Backward Defect Indicator (BDI) PM condition applies to TXP cards and MXP cards when 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 a PORT-CODE-MISM, page 2-130, occurs upstream.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: Clear the ODUK-BDI-PM Condition

Step 1   Complete the "Clear the OTUK-BDI condition" procedure on page 2-123.

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

2.6.167 ODUK-LCK-PM

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

The ODUK Locked Defect (LCK) PM condition applies to TXP and MXP cards when 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.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: 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/tac for more information or call TAC (1-800-553-2447).

2.6.168 ODUK-OCI-PM

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

The ODUK Open Connection Indication (OCI) PM condition applies to TXP cards and MXP cards when 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, page 2-120, downstream.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: 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/tac for more information or call TAC (1-800-553-2447).

2.6.169 ODUK-SD-PM

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

The ODUK Signal Degrade (SD) PM condition applies to TXP cards and MXP cards when G.709 monitoring is enabled. ODUK-SD-PM 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 path monitoring area of the optical data unit frame overhead.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: Clear the ODUK-SD-PM Condition

Step 1   Complete the "Clear the SD Condition" procedure on page 2-140.

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

2.6.170 ODUK-SF-PM

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

The ODUK Signal Fail (SF) PM condition (ODUK-SD-PM) applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, or MXP_2.5G_10G cards when ITU-T G.709 monitoring is enabled. ODUK-SF-PM indicates that incoming signal quality is poor and the incoming line BER has passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: Clear the ODUK-SF-PM Condition

Step 1   Complete the "Clear the SF Condition" procedure on page 2-142.

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

2.6.171 ODUK-TIM-PM

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

The ODUK Trace Identifier Mismatch (TIM) PM condition applies to the path monitoring area of the optical transport network (OTN) overhead for TXP cards and MXP cards. The condition occurs when there is a trace identifier mismatch in the data stream. ODUK-TIM-PM causes an ODUK-BDI-PM, page 2-120, downstream.

The ODUK-TIM-PM condition applies to TXP cards and MXP cards when 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.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: Clear the ODUK-TIM-PM Condition

Step 1   Complete the "Clear the TIM-P Alarm" procedure on page 2-156.

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

2.6.172 OTUK-AIS

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

The Optical Transport Unit (OTUK) AIS condition applies to transponder (TXP) cards and muxponder (MXP) cards when G.709 monitoring is enabled for the cards. OTUK-AIS is a secondary condition that indicates a more serious condition such as an LOS (OC-N), page 2-105, is occurring downstream. OTUK-AIS is reported in the optical transport unit overhead of the digital wrapper.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: Clear the OTUK-AIS Condition

Step 1   Complete the "Clear the AIS Condition" procedure on page 2-21.

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

2.6.173 OTUK-BDI

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

The OTUK BDI condition applies to TXP cards and MXP cards when 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, page 2-141, upstream. OTUK-BDI is triggered by a OTUK-TIM, page 2-125.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: Clear the OTUK-BDI condition

Step 1   Verify whether upstream nodes have an OTUK-AIS, page 2-123.

Step 2   In the upstream node, click the MXP or TXP card in the node view to display the card view.

Step 3   Click the **Provisioning > OTN > Trail Trade 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/tac for more information or call TAC (1-800-553-2447).

2.6.174 OTUK-IAE

- Major (MJ), Service Affecting (SA)

The OTUK Incoming Alignment Error (IAE) alarm applies to TXP cards and MXP cards when G.709 monitoring is enabled for the cards. OTUK-IAE refers to a single bit that allows the input port to notify the output port that the incoming signal has an alignment error. The error is indicated in the section monitoring overhead of the digital wrapper.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: Clear the OTUK-IAE Condition

Step 1   OTUK-IAE indicates an internal problem in the reporting card. Complete the "Physically Replace a Card" procedure on page 2-169.

⚠

Caution   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

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

2.6.175 OTUK-LOF

- Critical (CR), Service Affecting (SA)

The OTUK-LOF alarm applies to TXP cards and MXP cards when 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.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: Clear the OTUK-LOF Alarm

Step 1   Complete the "Clear the LOF (OC-N) Alarm" procedure on page 2-96.

Step 2   If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call TAC to report a service-affecting problem (1-800-553-2447).

2.6.176 OTUK-SD

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

The OTUK-SD condition applies to TXP cards and MXP cards when 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.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: Clear the OTUK-SD Condition

Step 1   Complete the "Clear the SD Condition" procedure on page 2-140.

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

2.6.177 OTUK-SF

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

The OTUK-SF condition applies to TXP cards and MXP cards when 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.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: Clear the OTUK-SF Condition

Step 1   Complete the "Clear the SD Condition" procedure on page 2-140.

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

2.6.178 OTUK-TIM

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

The OTUK-TIM alarm applies to TXP cards and MXP cards when 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, page 2-120.

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 cards to enable G.709 monitoring, refer to the *Cisco ONS 15454 Procedure Guide*.

Procedure: Clear the OTUK-TIM Alarm

Step 1 Complete the "Clear the TIM-P Alarm" procedure on page 2-156.

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

2.6.179 PDI-P

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

A PDI Path condition indicates a signal label mismatch failure (SLMF). An invalid signal label C2 byte in the SONET path overhead causes an SLMF. The C2 byte tells the equipment what the SONET payload envelope contains and how it is constructed. It enables a SONET device to transport multiple types of services.

The ONS 15454 encounters an SLMF when the payload, such as an ATM, does not match what the signal label is reporting. An AIS, 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 might result from the end-to-end Ethernet link integrity feature of the G1000-4. If the link integrity is the cause, it typically is accompanied by an TPTFAIL (G-Series), page 2-156, or a CARLOSS (G-Series), page 2-39, 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 might result from the end-to-end Ethernet link integrity feature of the ML-series card. If the link integrity is the cause, it typically is accompanied by a TPTFAIL (G-Series) reported against one or both packet over SONET (POS) ports terminating the circuit. If TPTFAIL is reported against one or both of 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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might 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.

Procedure: 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 **State** column lists the port as active.

   c.   If the State 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/tac for more information or call 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 2-167.

⚠️

Caution   Deleting a circuit might 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 2-169 for the optical/electrical (traffic) cards.

⚠️

Caution   Removing a card that currently caries 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. Consult 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 9   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.180 PEER-NORESPONSE

- Major (MJ), Non-Service Affecting (NSA)

The switch agent raises a Peer Card Not Responding alarm if either traffic card in a protection group does not receive a response to the peer status request message. PEER-NORESPONSE is a software failure and occurs at the task level, as opposed to a communication failure, which is a hardware failure between peer cards.

Procedure: Clear the PEER-NORESPONSE Alarm

Step 1   Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 for the reporting card.

- While the card resets, the FAIL LED on the physical card blinks and turns off.
- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 2   Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 3   Complete the "Reset a Traffic Card in CTC" procedure on page 2-169 for the reporting card.

- While the card resets, the FAIL LED on the physical card blinks and turns off.
- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 4   Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 5   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.181 PLM-P

- Critical (CR), Service Affecting (SA)

A Payload Label Mismatch Path 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, 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 will transmit this value, but a DS-3 card will transmit 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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might 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.

Procedure: Clear the PLM-P Alarm

Step 1   Verify that all circuits terminating in the reporting card are active:

a.   Click the **Circuits** tab.

b.   Verify that the **State** column lists the port as active.

c.   If the State 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

Step 2   After determining the port is active, verify the signal source to the traffic card reporting the alarm with an optical test set according to site specific practice.

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

Step 3   If traffic is being affected, complete the "Delete a Circuit" procedure on page 2-167.

Caution   Deleting a circuit might 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 the circuit deletion and recreation does not clear the alarm, verify the far-end OC-N card that provides STS payload to the DS-N card.

Step 6   If the alarm does not clear, verify the cross-connect between the OC-N card and the DS-N card.

Step 7   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*.

Step 8   If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the reporting traffic card.

⚠

Caution   Removing a card that currently caries 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. Consult 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 9   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.182 PLM-V

   • Minor (MN), Service Affecting (SA)

A Payload Label Mismatch VT Layer alarm indicates that the content of the V5 byte in the SONET overhead is inconsistent or invalid. PLM-V occurs when ONS nodes interoperate with equipment that performs bit-synchronous mapping for DS-1. ONS nodes use asynchronous mapping.

Procedure: 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.183 PORT-CODE-MISM

   • Major (MJ) Non-Service Affecting (NSA)

The Pluggable Port Security Code Mismatch alarm refers to ML-series Ethernet (traffic) cards, MXPs, and TXPs. PORT-CODE-MISM occurs when the SFP connector that is plugged into the card is not supported by Cisco.

Procedure: 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/tac for more information or call TAC (1-800-553-2447).

2.6.184 PORT-COMM-FAIL

- Major (MJ), Service Affecting (SA)

The Port Communication Failure alarm applies to TXP and MXP card SFPs. It occurs when the card cannot communicate with the SFP.

Procedure: Clear the PORT-COMM-FAIL Alarm

Step 1   Replace the faulty SFP with a new SFP:

    a.   Unplug the SFP connector and fiber from the ML-series Ethernet (traffic) card.

    b.   If the SFP connector has a latch securing the fiber cable, pull the latch upward to release the cable.

    c.   Pull the fiber cable straight out of the connector.

    d.   Plug the fiber into a Cisco-supported SFP connector.

    e.   If the new SFP connector has a latch, close the latch over the cable to secure it.

    f.   Plug the cabled SFP connector into the ML-series Ethernet card port until it clicks.

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

2.6.185 PORT-MISMATCH

- Major (MJ), Non-Service Affecting (NSA)

The Pluggable Port Mismatch alarm applies to ML-series Ethernet (traffic) 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*. If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.186 PORT-MISSING

- Major (MJ), Non-Service Affecting (NSA)

The Pluggable Port Code 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*.

Procedure: 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/tac for more information or call TAC (1-800-553-2447).

2.6.187 PRC-DUPID

- Major (MJ), Service Affecting (SA) for Ring
- Major (MJ), Non-Service Affecting (NSA) for NE

The Procedural Error Duplicate Node ID alarm indicates that two identical node IDs exist in the same ring. The ONS 15454 requires each node in the ring to have a unique node ID.

Procedure: 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 Ring ID or Node ID Number" procedure on page 2-164.

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 Node ID Number" procedure on page 2-164 so that each node ID is unique.

Step 5   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.188 PROTNA

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

The Protection Unit Not Available alarm is caused by an OOS protection card when a TCC+/TCC2 or 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.

Procedure: 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 (TCC+/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 a 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 2-169 for the reporting card.

- While the card resets, the FAIL LED on the physical card blinks and turns off.

- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 4   Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms window in CTC.

- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.

- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 5   If the alarm does not clear, complete the "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168 for the reporting card.

Step 6   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.189 PWR-A

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

The NE Power (PWR) Failure At Connector A alarm applies to the NE shelf. It occurs when there is no power supplied to the main power connector. PWR-A can occur if power is connected to the backup power connector (Connector B) but not to Connector A, because power must be applied to both supplies.

Warning   **Hazardous energy level available at the power source and power connection. Do not bridge across battery terminals or bridge battery terminal to ground; metal objects heat up and can cause serious burns or weld the metal object to the terminals.**

Procedure: Clear the PWR-A Alarm

Step 1   Ensure that a power connection is present between the power source and power connector A.

Step 2   If necessary, reseat the connections between the source and the power connector A.

Step 3   If the alarm does not clear, verify the continuity of the power connection with a voltmeter using the "Measure Voltage" task in the *Cisco ONS 15454 Procedure Guide*.

Step 4   If the alarm does not clear, verify the source power output with a voltmeter using the "Measure Voltage" task in the *Cisco ONS 15454 Procedure Guide*.

Step 5   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.190 PWR-B

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

The NE Power Failure at Connector B alarm applies to the NE rack. It occurs when there is no power supplied to the backup power connector. PWR-B can occur if power is connected to the main power connector (Connector A) but not to Connector B, because power must be applied to both supplies.

Warning   **Hazardous energy level available at the power source and power connection. Do not bridge across battery terminals or bridge battery terminal to ground; metal objects heat up and can cause serious burns or weld the metal object to the terminals.**

Procedure: Clear the PWR-B Alarm

Step 1   Ensure that a power connection is present between the power source and power connector B.

Step 2   If necessary, reseat the connections between the source and power connector B.

Step 3   If the alarm does not clear, verify the continuity of the power connection with a voltmeter using the "Measure Voltage" task in the *Cisco ONS 15454 Procedure Guide*.

Step 4   If the alarm does not clear, verify the source power output with a voltmeter using the "Measure Voltage" task in the *Cisco ONS 15454 Procedure Guide*.

Step 5   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.191 PWR-REDUN

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

The Redundant Power Capability Lost 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.

Procedure: Clear the PWR-REDUN Alarm

Step 1   The card fuse is not field-replaceable. Complete the "Physically Replace a Card" procedure on page 2-169.

⚠

Caution   Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

Step 2   Log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447) to arrange a card return for service.

2.6.192 RAI

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

The Remote Alarm Indication condition signifies an end-to-end failure. The error condition is sent from one end of the SONET path to the other. RAI on the DS3XM-6 card indicates that the far-end node is receiving a DS-3 AIS, page 2-21.

Procedure: Clear the RAI Condition

Step 1   Complete the "Clear the AIS Condition" procedure on page 2-21.

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

2.6.193 RCVR-MISS

   • Major (MJ), Service Affecting (SA)

A Facility Termination Equipment Receiver Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance usually occurs when a receive cable is missing from 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.

Procedure: 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 OK, verify that the cabling is securely connected.

Step 3   If the cabling is OK, 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.194 RFI-L

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

A Remote Fault Indication (RFI) Line 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-L condition in the reporting node. RFI-L indicates that the condition is occurring at the line level.

Procedure: 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 LOS (OC-N), page 2-105.

Step 3   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.195 RFI-P

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

An RFI Path 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-P condition in the reporting node. RFI-P occurs in the node that terminates a path.

Procedure: Clear the RFI-P Condition

Step 1   Verify that the ports are enabled and in service (IS) on the reporting ONS 15454:

    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 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 an UNEQ-P, page 2-159, or UNEQ-V, page 2-161.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.196 RFI-V

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

An RFI VT Layer condition occurs when the ONS 15454 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-V condition in the reporting node. RFI-V indicates that an upstream failure has occurred at the VT layer.

⚠️

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.

Procedure: 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 an UNEQ-P, page 2-159, or UNEQ-V, page 2-161.

Step 6 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.197 RING-MISMATCH

- Major (MJ), Service Affecting (SA)

A Procedural Error Mismatch Ring alarm occurs when the ring ID of the ONS 15454 that is reporting the alarm does not match the ring ID of another ONS node in the BLSR. ONS nodes connected in a BLSR must have identical ring IDs to function.

Procedure: Clear the RING-MISMATCH Alarm

Step 1   In the node view, click the **Provisioning > BLSR** tabs.

Step 2   Note the number in the Ring ID field.

Step 3   Log into the next ONS node in the BLSR.

Step 4   Complete the "Identify a Ring ID or Node ID Number" procedure on page 2-164.

Step 5   If the ring ID matches the ring ID in the reporting ONS node, repeat Step 4 for the next ONS node in the BLSR.

Step 6   Complete the "Change a Ring ID Number" procedure on page 2-164.

Step 7   Verify that the ring map is correct.

Step 8   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.198 RING-SW-EAST

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

The Ring Switch Is Active East Side 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.

2.6.199 RING-SW-WEST

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

The Ring Switch Is Active West Side 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.

2.6.200 RSVP-HELLODOWN

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

The Resource Reservation Protocol (RSVP) Hello Down alarm 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.

Procedure: 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:

    a. In the 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.201 RUNCFG-SAVENEED

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

The Run Configuration Save Needed 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.

2.6.202 SD

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

A Signal Degrade (SD) condition occurs when the quality of the signal is so poor that the bit error rate on the incoming optical line passed the signal degrade threshold. Signal degrade is defined by Telcordia as a soft failure condition. SD and 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-L causes a switch from the working card to the protect card at the line (facility) level. A line or facility level SD condition travels on the B2 byte of the SONET overhead.

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.

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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might 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.

Procedure: Clear the SD Condition

Step 1   Complete the "Verify BER Threshold Level" procedure on page 2-169.

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 OK, verify that optical receive levels are within the acceptable range.

Step 4   If receive levels are OK, 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 might be failing and require replacement.

Step 8   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.203 SD-L

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

An SD Line condition is similar to an SD, page 2-139. It applies to the line level of the SONET signal

Procedure: Clear the SD-L Condition

Step 1   Complete the "Clear the SD Condition" procedure on page 2-140.

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

2.6.204 SD-P

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

An SD Path condition is similar to an SD, page 2-139, 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 protection configuration 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 configuration, an SD-P condition causes a switch from the working card to the protect card at the path (STS) level. On BLSR 1+1 or 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 bit error rate 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.

Procedure: Clear the SD-P Condition

Step 1   Complete the "Clear the SD Condition" procedure on page 2-140.

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

2.6.205 SF

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

A Signal Fail (SF) condition 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, page 2-139, and SF 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.

SF-L causes a switch from the working card to the protect card at the line (facility) level. A line or facility level SF condition travels on the B2 byte of the SONET overhead.

SF causes a card to switch from working to protect at either the path or line level. The SF 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.

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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might 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.

Procedure: Clear the SF Condition

Step 1   Complete the "Clear the SD Condition" procedure on page 2-140.

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

2.6.206 SF-L

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

An SF Line condition is similar to an SF, page 2-141, but it applies to the line layer of the signal.

Procedure: Clear the SF-L Condition

Step 1   Complete the "Clear the SD Condition" procedure on page 2-140.

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

2.6.207 SF-P

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

An SF Path condition is similar to an , 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 protection configuration circuits, the BER threshold on the ONS 15454 is user provisionable and has a range for SF from 10^{-5} to 10^{-3}. For BLSR 1+1 or unprotected circuits, the BER threshold value is not user provisionable and the error rate is hard-coded to 10^{-3}.

For path protection configuration, SF-P causes a switch from the working card to the protect card at the path (STS) level. For BLSR 1+1 or unprotected circuits, SF-P 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.

Procedure: Clear the SF-P Condition

Step 1   Complete the "Clear the SD Condition" procedure on page 2-140.

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

2.6.208 SFTWDOWN

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

A Software Download in Progress alarm occurs when the TCC+/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/tac for more information or call TAC (1-800-553-2447).

⚠️

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

✎

Note   SFTWDOWN is an informational alarm.

2.6.209 SNTP-HOST

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

The Simple Network Timing Protocol (SNTP) Host Failure alarm 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.

Procedure: 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 might 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/tac for more information or call TAC (1-800-553-2447).

2.6.210 SPAN-SW-EAST

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

The Span Switch Is Active East Side 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.

2.6.211 SPAN-SW-WEST

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

The Span Switch Is Active West Side 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.

2.6.212 SQUELCH

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

The Ring Squelching Traffic condition occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance FORCE RING commands. The isolation or failure of the node disables circuits that originate or terminate on the failed node. Squelch alarms appear on one or both of the nodes on either side of the isolated/failed node. AIS-P, 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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Procedure: Clear the SQUELCH Condition

Step 1   Determine the isolated node:

   a.   In the node view, click **View > Go to Network View**.

   b.   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 OK, verify that the proper ports are 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 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 OK, ensure that the optical transmit and receive fibers are connected properly.

Step 7 If the connectors are OK, complete the "Physically Replace a Card" procedure on page 2-169 for the OC-N card.

⚠

Caution Removing a card that currently caries 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. Consult the *Cisco ONS 15454 Procedure Guide* for information.

Step 8 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.213 SQUELCHED

- Major (MJ), Service Affecting (SA)

The DWDM Client Signal Squelched alarm is raised by an MXP or TXP card when G.709 monitoring is enabled and the card is operating in transparent mode. The alarm occurs on a far-end MXP or TXP client port when the near end detects an LOF (OC-N), page 2-96, or LOS (OC-N), page 2-105. The signal loss is indicated by an OTUK-AIS, page 2-123, in the OTN overhead. SQUELCHED can also indicate that the far-end trunk signal is invalid.

Procedure: Clear the SQUELCHED Alarm

Step 1 Verify that the far-end node and near-end node are not reporting an LOF (OC-N), page 2-96, or an LOS (OC-N), page 2-105. If so, complete the "Clear the LOF (OC-N) Alarm" procedure on page 2-96.

Step 2 If no LOF or LOS is reported, verify that the far-end node and near-end are not reporting a WVL-MISMATCH, page 2-162, for the trunk or DSP-FAIL, page 2-55. If either alarm is reported, complete the "Clear the WVL-MISMATCH alarm" procedure on page 2-162 or the "Clear the DSP-FAIL Alarm" procedure on page 2-55 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:

   a. Double-click the client card to display the card view.

   b. Click the **Maintenance > Loopback** tabs.

   c. 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 will also clear any loopback provisioned on the port.

Step 4 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.214 SSM-DUS

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

The Synchronization Status (SSM) Message Quality Changed to Do-Not-Use (DUS) condition occurs when the synchronization status message (SSM) quality level degrades to DUS or is manually changed to DUS.

The signal is often manually changed to DUS to prevent timing loops from occurring. Sending a DUS prevents the timing from being reused in a loop. The DUS signal can also be sent for line maintenance testing.

Note   SSM-DUS is an informational condition. It does not require troubleshooting.

2.6.215 SSM-FAIL

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

The SSM Failed alarm occurs when the synchronization status messaging received by the ONS 15454 fails. The problem is external to ONS 15454. The ONS 15454 is set up to receive SSM, but the timing source is not delivering valid SSM messages.

Procedure: 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.

If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.216 SSM-LNC

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

The SSM Local Node Clock (LNC) Traceable condition occurs when the SSM (S1) byte of the SONET overhead multiplexing section has been changed to signify that the line or BITS timing source is LNC.

Note   SSM-LNC is an informational condition. It does not require troubleshooting.

2.6.217 SSM-OFF

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

Cisco ONS 15454 Troubleshooting Guide, R4.0

The SSM Off condition applies to references used for timing the node. It occurs when the SSM for the reference has been turned off. The ONS 15454 is set up to receive SSM, but the timing source is not delivering SSM messages.

Procedure: Clear the SSM-OFF Condition

Step 1   Complete the "Clear the SSM-FAIL Alarm" procedure on page 2-147.

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

2.6.218 SSM-PRC

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

The SSM Primary Reference Clock (PRC) Traceable condition occurs when the SONET transmission level is changed to PRC.

Note   SSM-PRC is an informational condition. It does not require troubleshooting.

2.6.219 SSM-PRS

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

The SSM Primary Reference Source (PRS) Traceable condition occurs when the SSM transmission level is changed to Stratum 1 Traceable.

Note   SSM-PRS is an informational condition. It does not require troubleshooting.

2.6.220 SSM-RES

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

The SSM Reserved (RES) For Network Synchronization Use condition occurs when the synchronization message quality level is changed to RES.

Note   SSM-RES is an informational condition. It does not require troubleshooting.

2.6.221 SSM-SMC

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

The SSM SONET Minimum Clock (SMC) Traceable condition occurs when the synchronization message quality level changes to SMC. The login node does not use the clock because the node cannot use any reference beneath its internal level, which is ST3.

Note   SSM-SMC is an informational condition. It does not require troubleshooting.

2.6.222 SSM-ST2

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

The SSM Stratum 2 (ST2) Traceable condition occurs when the synchronization message quality level is changed to ST2.

Note   SSM-ST2 is an informational condition. It does not require troubleshooting.

2.6.223 SSM-ST3

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

The SSM Stratum 3 (ST3) Traceable condition occurs when the synchronization message quality level is changed to ST3.

Note   SSM-ST3 is an informational condition. It does not require troubleshooting.

2.6.224 SSM-ST3E

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

The SSM Stratum 3E (ST3E) Traceable condition indicates that the synchronization message quality level is changed to ST3E from a lower level of synchronization. SSM-ST3E is a Generation 2 SSM and is not used for Generation 1.

Note   SSM-ST3E is an informational condition. It does not require troubleshooting.

2.6.225 SSM-ST4

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

The SSM Stratum 4 (ST4) Traceable condition occurs when the synchronization message quality level is lowered to ST4. The message quality is not used because it is below ST3.

Note   SSM-ST4 is an informational condition. It does not require troubleshooting.

2.6.226 SSM-STU

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

The SSM Synchronization Traceability Unknown (STU) condition occurs when the reporting node is timed to a reference that does not support SSM, but the ONS 15454 has SSM support enabled. STU can also occur if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15454.

Procedure: Clear the STU Condition

Step 1   In the node view, click the **Provisioning > Timing** tabs.

Step 2   If **Sync Messaging** is checked, deselect the box.

Step 3   If **Sync Messaging** is unchecked, check the box.

Step 4   Click **Apply**.

Step 5   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.227 SSM-TNC

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

The SSM Transit Node Clock (TNC) Traceable condition occurs when the synchronization message quality level is changed to TNC.

> **Note**   SSM-TNC is an informational condition. It does not require troubleshooting.

2.6.228 SWMTXMOD

- Critical (CR), Service Affecting (SA)

The Switching Matrix Module Failure alarm occurs on the 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 might lose traffic as a result of the cross-connect frame failure.

Procedure: Clear the SWMTXMOD Alarm

Step 1   If the card reporting the alarm is the standby cross-connect card, complete the "Reset a Traffic Card in CTC" procedure on page 2-169 for the card.

- While the card resets, the FAIL LED on the physical card node blinks and turns off.

- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 2 Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms window in CTC.

- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.

- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 3 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 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 Cross-Connect Cards" procedure on page 2-166.

> ✎
> **Note**   After the active cross-connect goes into standby, the original standby slot becomes active. The former standby card ACT/STBY 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 2-169 for the reporting card.

- While the card resets, the FAIL LED on the physical card node blinks and turns off.

- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 6 Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms window in CTC.

- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.

- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 7 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 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 Cross-Connect Cards" procedure on page 2-166.

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 2-169 for the reporting card.

- While the card resets, the FAIL LED on the physical card node blinks and turns off.

- While the card resets, the white LED with the letters "LDG" appears on the reset card in CTC.

Step 10 Verify that the reset is complete and error-free.

- No new alarms appear in the Alarms window in CTC.

- If you are looking at the physical ONS 15454, the ACT/STBY LED is illuminated.

- If you are looking at the node view of the ONS 15454, an amber LED depiction with "Sby" has replaced the white "LDG" depiction on the card in CTC.

Step 11 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-170 for the traffic line card.

Step 12 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.229 SWTOPRI

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

The Synchronization Switch to Primary Reference condition occurs when the ONS 15454 switches to the primary timing source (reference 1). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

✎
Note   SWTOPRI is an informational condition. It does not require troubleshooting.

2.6.230 SWTOSEC

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

The Synchronization Switch to Secondary Reference condition occurs when the ONS 15454 has switched to the secondary timing source (reference 2). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Procedure: Clear the SWTOSEC Condition

Step 1   To clear the condition, clear alarms related to failures of the primary source, such as SYNCPRI, page 2-153.

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

2.6.231 SWTOTHIRD

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

The Synchronization Switch to Third Reference condition occurs when the ONS 15454 has switched to the third timing source (reference 3). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Procedure: Clear the SWTOTHIRD Condition

Step 1   To clear the condition, clear alarms related to failures of the primary source, such as SYNCPRI, page 2-153, or SYNCSEC, page 2-154.

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

2.6.232 SYNC-FREQ

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

The Synchronization Reference Frequency Out Of Bounds condition is reported against any reference that is out of the bounds for valid references. The login node fails the reference and chooses another internal or external reference to use.

Procedure: 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 2-169 for the TCC+/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 TCC+/TCC2 to transfer the system software to the newly installed TCC+/TCC2. Software transfer occurs in instances where different software versions exist on the two cards. During the transfer operation, the LEDs on the TCC+/TCC2 flash fail and then the active/standby LED flashes. When the transfer completes, the TCC+/TCC2 reboots and goes into standby mode after approximately three minutes.

Step 3 If the SYNC-FREQ condition continues to report after replacing the TCC+/TCC2 card, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.233 SYNCPRI

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

A Loss of Timing on Primary Reference alarm occurs when the ONS 15454 loses the primary timing source (reference 1). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the ONS 15454 should switch to its secondary timing source (reference 2). Switching to the secondary timing source also triggers SWTOSEC, page 2-152.

Procedure: Clear the SYNCPRI Alarm

Step 1 In the 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 2-101.

Step 4   If the primary reference clock is an incoming port on the ONS 15454, complete the "Clear the LOS (OC-N) Alarm" procedure on page 2-105.

Step 5   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.234 SYNCSEC

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

A Loss of Timing on Secondary Reference alarm occurs when the ONS 15454 loses the secondary timing source (reference 2). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCSEC occurs, the ONS 15454 should switch to the third timing source (reference 3) to obtain valid timing for the ONS 15454. Switching to the third timing source also triggers SWTOTHIRD, page 2-152.

Procedure: Clear the SYNCSEC Alarm

Step 1   In the 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 2-101.

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 (OC-N) Alarm" procedure on page 2-105.

Step 6   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.235 SYNCTHIRD

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

A Loss of Timing on Third Reference alarm occurs when the ONS 15454 loses the third timing source (reference 3). The ONS 15454 uses three ranking timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCTHIRD occurs and the ONS 15454 uses an internal reference for source three, the TCC+/TCC2 card might have failed. The ONS 15454 often reports either FRNGSYNC, page 2-82, or HLDOVRSYNC, page 2-87, 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.

Procedure: 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 2-101.

Step 4   If the third timing source is an incoming port on the ONS 15454, complete the "Clear the LOS (OC-N) Alarm" procedure on page 2-105.

Step 5   If the third timing source uses the internal ONS 15454 timing, complete the "Reset Active TCC+/TCC2 Card and Activate Standby Card" procedure on page 2-168.

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 TAC (1-800-553-2447). If the TAC technician tells you to reseat the card, complete "Remove and Reinsert (Reseat) the Standby TCC+/TCC2" procedure on page 2-168. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-169.

2.6.236 SYSBOOT

- Major (MJ), Service Affecting (SA)

The System Reboot alarm indicates that new software is booting on the TCC+/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/tac for more information or call 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.

2.6.237 TIM-P

- Critical (CR), Service Affecting (SA) for STSTERM
- Minor (MN), Non-Service Affecting (NSA) for STSMON

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 (OC-N) alarm (see page 2-105), the UNEQ-P alarm (see page 2-159), or the PLM-P alarm (see page 2-128). If these alarms accompany TIM-P, reattach or replace the original cables/fibers to clear the alarms.

Procedure: Clear the TIM-P Alarm

Step 1   Log into the circuit source node and click the **Circuits** tab.

Step 2   Select the circuit reporting the alarm, 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** from the shortcut menu.

Step 5   On the detailed circuit map, right-click the drop/destination circuit port and choose **Edit Path Trace** from the shortcut menu.

Step 6   Compare the Current Transmit String and the Current Expected String entries in the Edit J1 Path Trace dialog box.

Step 7   If the strings differ, correct the Transmit or Expected strings and click **Apply**.

Step 8   Click **Close**.

Step 9   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.238 TPTFAIL (G-Series)

- Major (MJ), Service Affecting (SA)

The Transport (TPT) Layer Failure alarm for the G-series 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 AIS-P, page 2-22; LOP-P, page 2-98; PDI-P, page 2-126, or UNEQ-P, page 2-159, 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 CARLOSS (G-Series), page 2-39, the C2 byte in the SONET path overhead indicates a PDI-P alarm. This, 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 condition 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.

Procedure: Clear the TPTFAIL (G-Series) 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 a PDI-P alarm is reported, the problem might 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.239 TPTFAIL (ML-Series)

- Major (MJ), Service Affecting (SA)

The TPT Layer Failure alarm for the ML-series 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 either the SONET path, the remote POS port, or a misconfiguration of the POS port which prevents the complete end-to-end POS path from working. If any SONET path alarms such as AIS-P, page 2-22; LOP-P, page 2-98; PDI-P, page 2-126, or UNEQ-P, page 2-159, exist on the circuit used by the POS port, the affected port might report a TPTFAIL alarm. If the far-end ML-series POS port is administratively disabled, it inserts an AIS-P condition 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 will cause the port to go down and report TPTFAIL.

Procedure: Clear the TPTFAIL (ML-Series) 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 PLM-P, page 2-128, 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 a PDI-P alarm is the only one reported against the POS port circuit and the circuit is terminated by a G-series card, verify whether CARLOSS (G-Series), page 39, is reported against the G-series card and if so, complete the "Clear the CARLOSS (G-Series) Alarm" procedure on page 2-40.

Step 4   If an AIS-P condition, an LOP-P alarm, or an UNEQ-P alarm 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.240 TRMT

- Major (MJ), Service Affecting (SA)

A Missing Transmitter alarm occurs when there is a transmit failure on the DS-1 card because of an internal hardware failure. The card must be replaced.

Procedure: Clear the TRMT Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-169 for the reporting DS-1 card.

⚠

Caution Removing a card that currently caries 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. Consult 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, call the Technical Assistance Center (TAC) at (1-800-553-2447) to discuss the failed card and possibly open a returned materials authorization (RMA).

2.6.241 TRMT-MISS

- Major (MJ), Service Affecting (SA)

A Facility Termination Equipment Transmitter Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance is detected when a transmit cable is missing on the DS-1 port or the backplane does not match the inserted card; for example, an SMB connector or a BNC connector 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.

Procedure: 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.242 UNC-WORD

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

The Uncorrected Forward Error Correction (FEC) Word condition indicates that forward error correction (FEC), which is used to lower signal to noise ratio by 7dB to 8dB, could not correct the frame sufficiently.

Procedure: Clear the UNC-WORD Condition

Step 1   Complete the "Clear the SD Condition" procedure on page 2-140.

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

2.6.243 UNEQ-P

- Critical (CR), Service Affecting (SA)

An SLMF UNEQ Path alarm occurs when the path does not have a valid sender. The UNEQ-P indicator is carried in the C2 signal path byte in the SONET overhead. The source of the problem is the node that is transmitting the signal into the node reporting the UNEQ-P.

The alarm might 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, an UNEQ-P alarm is reported on the OC-N cards and an AIS-P, 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.

Procedure: Clear the UNEQ-P Alarm

Step 1   In the node view, click **View > Go to Network View**.

Step 2   Right-click the alarm to display the Select Affected Circuits dialog box.

Step 3   Click the Select Affected Circuits dialog box.

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 might 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.

   a. Click the VT tunnel circuit row to highlight it. Complete the "Delete a Circuit" procedure on page 2-167.

   b. If an error message dialog box appears, the VT tunnel is valid and not the cause of the alarm.

   c. If any other columns contain VTT, repeat Step 6.

Step 7   If all ONS nodes in the ring appear in the CTC network view, verify whether the circuits are complete:

   a. Click the **Circuits** tab.

   b. Verify that INCOMPLETE is not listed in the State 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 2-167.

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:

   a. Click the **Circuits** tab.

   b. Verify that the **State** 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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might result in hazardous radiation exposure.**

Step 13   If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-169 for the OC-N and DS-N cards.

⚠️

Caution   Removing a card that currently caries 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. Consult 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 14   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.244 UNEQ-V

 • Major (MJ), Service Affecting (SA)

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 might 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 might pose an eye hazard. Use of controls or adjustments or performance of procedures other than those specified might 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.

Procedure: Clear the UNEQ-V Alarm

Step 1   Complete the "Clear the UNEQ-P Alarm" procedure on page 2-159.

Step 2   If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.245 WKSWPR

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

The Working Switched To Protection condition occurs when a line experiences an LOS (OC-N), page 2-105; an SF, page 2-141, or an SD, page 2-139.

Procedure: Clear the WKSWPR Condition

Step 1   Complete the "Clear the LOS (OC-N) Alarm" procedure on page 2-105.

Step 2   If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.6.246 WTR

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

The Wait To Restore condition occurs when WKSWPR, page 2-162, is raised the wait-to-restore time has not expired, meaning 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.

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

2.6.247 WVL-MISMATCH

- Major (MJ), Service Affecting (SA)

The Equipment Wavelength Mismatch alarm applies to the TXP and MXP cards. It occurs when you provision the card in CTC with a wavelength that the card does not support.

Procedure: Clear the WVL-MISMATCH alarm

Step 1   In node view, double-click the TXP or MXP 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:

   a.   In the node view, click the **Inventory** tab.

   b.   Locate the slot where the TXP or MXP 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 the 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/tac for more information or call TAC to report a service-affecting problem (1-800-553-2447).

2.7 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 2-8   DS3-12E Line Alarms

Alarm	UNFRAMED	M13	CBIT
LOS	◆	◆	◆
AIS	◆	◆	◆
LOF	○	◆	◆
IDLE	○	◆	◆
RAI	○	◆	◆
Terminal Lpbk	◆	◆	◆
Facility Lpbk	◆	◆	◆
FE Lpbk	○	○	◆
FE Common Equipment Failure	○	○	◆
FE Equipment Failure-SA	○	○	◆
FE LOS	○	○	◆
FE LOF	○	○	◆
FE AIS	○	○	◆
FE IDLE	○	○	◆
FE Equipment Failure-NSA	○	○	◆

2.8 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.

Procedure: Identify a Ring ID 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 the node view, click **View > Go to Network View**.

Step 3   Click the **Provisioning > BLSR** tabs.

From the Ring ID column, record the Ring ID, 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.

Procedure: Change a Ring ID Number

Step 1   Log into a node on the network. If you are already logged in, go to Step 2.

Step 2   In the 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 ID in the Ring ID field.

Step 6   Click **Apply**.

Step 7   Click **Yes** at the Changing Ring ID dialog box.

Procedure: Change a 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 the 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**.

Procedure: 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 the 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**.

Procedure: Verify or Create Node DCC Terminations

Step 1   Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2   In the node view, click the **Provisioning > DCC/GCC** 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**.

Procedure: 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 the 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 SPAN** and click **Apply**.

Step 5   Click **OK** on the BLSR Operations dialog box.

Procedure: Clear a BLSR Span Lock Out

Step 1   Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2   In the 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.

Procedure: Clear a Path Protection Lock Out

Step 1   Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2   In the 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.

Procedure: 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 the node view.

Step 3   In the node view, click the **Maintenance > Protection** tabs.

Step 4   Double-click the protection group that contains the reporting card.

Step 5   Click the Working or active card of the selected groups.

Step 6   Click **Switch** and **Yes** in the Confirmation dialog box.

Procedure: Side Switch the Active and Standby 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 the node view.

Step 3   Determine the active or standby cross-connect card.

The ACT/STBY LED of the active card is green. The ACT/STBY 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 > XC > Cards** tabs.

Step 5   Click **Switch**.

Step 6   Click **Yes** in the Confirm Switch dialog box.

Procedure: Clear 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   In the 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** at the confirmation dialog box.

Procedure: 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** at the Delete Circuits dialog box.

Procedure: Clear a 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**.

Procedure: Reset Active TCC+/TCC2 Card and Activate Standby Card

⚠️

Caution   The TCC+ or 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 TCC+/TCC2 card.

If you are looking at the physical ONS 15454, the ACT/STBY LED of the active TCC+/TCC2 is green. The ACT/STBLY LED of the standby TCC+/TCC2 is amber.

Step 3   Right-click the active TCC+/TCC2 card in CTC.

Step 4   Choose **Reset Card** from the shortcut menu.

Step 5   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.

Step 6   Verify that the reset is complete and error-free.

Double-click the node and ensure that the reset TCC+/TCC2 card is in standby mode and that the other TCC+/TCC2 card is active.

- If you are looking at the physical ONS 15454, the ACT/STBY LED of the active TCC+/TCC2 is green. The ACT/STBLY LED of the standby TCC+/TCC2 is amber.
- No new alarms appear in the Alarms window in CTC.
- If you are looking at the physical ONS 15454, the active TCC+/TCC2 ACT/STBY LED is green, and the LED of the standby TCC+/TCC2 is amber.

Procedure: Remove and Reinsert (Reseat) the Standby TCC+/TCC2

⚠️

Caution   Do not perform this action without the supervision and direction of the Cisco Technical Assistance Center (TAC). The Cisco TAC can be reached at (1-800-553-2447).

⚠️

Caution   The TCC+ or TCC2 card reseat can be traffic-affecting.

✎

Note   Before you reset the TCC+ or 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 TCC+/TCC2 you want to reset is in standby mode. On the TCC+/TCC2 card, the ACT/STBY (Active/Standby) LED is amber when the TCC+/TCC2 is in standby mode.

Step 3   When the TCC+/TCC2 is in standby mode, unlatch both the top and bottom ejector levers on the TCC+/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 ejector levers.

> ✎
> **Note**   The TCC+/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 TCC+/TCC2 card reboots.

Procedure: Reset a Traffic Card in CTC

Step 1   Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2   In node view, position the cursor over the multispeed slot (Slots 1 to 4 and 14 to 17) or high-speed slot (Slots 5,6 and 12 and 13) reporting the alarm.

Step 3   Right-click and choose **RESET CARD** from the shortcut menu.

Step 4   Click **Yes** in the Are You Sure dialog box.

Procedure: 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 the 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**.

Procedure: Physically Replace a Card

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.

Procedure: 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.

Procedure: 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.