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 commonly encountered Cisco ONS 15327 alarms and conditions. Table 2-1 on page 2-2 through Table 2-4 on page 2-3 give lists of ONS 15327 alarms organized by severity. Table 2-5 on page 2-4 gives a list of alarm organized alphabetically. Table 2-6 on page 2-6 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 15327 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 15327 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

BKUPMEMP, page 2-30	HITEMP, page 2-72	MEA (EQPT), page 2-90
COMIOXC, page 2-37	IMPROPRMVL, page 2-73	MFGMEM, page 2-92
CTNEQPT-PBPROT, page 2-41	LOF (DS-3), page 2-79	PLM-P, page 2-95
CTNEQPT-PBWORK, page 2-43	LOF (OC-N), page 2-79	SWMTXMOD, page 2-114
EQPT, page 2-50	LOP-P, page 2-80	TIM-P, page 2-119
EQPT-MISS, page 2-51	LOS (DS-3), page 2-83	UNEQ-P, page 2-122
FAN, page 2-59	LOS (OC-N), page 2-84	

2.1.2 Major Alarms (MJ)

Table 2-2 lists Major alarms.

Table 2-2 Major Alarm Index

APSCM, page 2-21	EOC, page 2-48	MEM-GONE, page 2-91
APSCNMIS, page 2-21	E-W-MISMATCH, page 2-51	PEER-NORESPONSE, page 2-94
BLSROSYNC, page 2-30	EXTRA-TRAF-PREEMPT, page 2-54	PRC-DUPID, page 2-96
CARLOSS (EQPT), page 2-31	FANDEGRADE, page 2-60	RCVR-MISS, page 2-101
CARLOSS (E Series), page 2-32	INVMACADR, page 2-76	RING-MISMATCH, page 2-103
CARLOSS (G Series), page 2-34	LOF (BITS), page 2-77	SYSBOOT, page 2-119
CONTBUS-A-18, page 2-37	LOF (DS-1), page 2-78	TPTFAIL (G-Series), page 2-120
CONTBUS-B-18, page 2-38	LOP-V, page 2-81	TRMT, page 2-121
CONTBUS-IO-A, page 2-39	LOS (BITS), page 2-81	TRMT-MISS, page 2-121
CONTBUS-IO-B, page 2-40	LOS (DS-1), page 2-82	UNEQ-V, page 2-124
DBOSYNC, page 2-45		

2.1.3 Minor Alarms (MN)

Table 2-3 lists Minor alarms.

Table 2-3 Minor Alarm Index

APSB, page 2-18	ELWBATVG-A, page 2-47	PWR-A, page 2-98
APSCDFLTK, page 2-19	ELWBATVG-B, page 2-47	PWR-B, page 2-99
APSC-IMP, page 2-20	EXCCOL, page 2-53	PWR-REDUN, page 2-100
APSCINCON, page 2-20	EXT, page 2-54	SFTWDOWN, page 2-107
APSMM, page 2-22	FEPRLF, page 2-68	SNTP-HOST, page 2-108
AUTORESET, page 2-25	FSTSYNC, page 2-71	SSM-FAIL, page 2-110
AUTOSW-LOP (STSMON), page 2-26	HITEMP, page 2-72	SYNCPRI, page 2-117

Table 2-3 Minor Alarm Index (continued)

AUTOSW-UNEQ (STSMON), page 2-27	MEM-LOW, page 2-92	SYNCSEC, page 2-117
DATAFLT, page 2-45	NOT-AUTHENTICATED, page 2-92	SYNCTHIRD, page 2-118
EHIBATVG-A, page 2-46	PLM-V, page 2-96	TIM-P, page 2-119
EHIBATVG-B, page 2-47	PROTNA, page 2-97	

2.1.4 Conditions (NA or NR)

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

Table 2-4 Conditions Index

AIS, page 2-16	FE-FRCDWKSWPR-SPAN, page 2-65	MANUAL-REQ-SPAN, page 2-90
AIS-L, page 2-16	FE-IDLE, page 2-66	PDI-P, page 2-93
AIS-P, page 2-17	FE-LOCKOUTOFPR-SPAN, page 2-66	RAI, page 2-100
AIS-V, page 2-17	FE-LOF, page 2-67	RFI-L, page 2-101
AS-CMD, page 2-23	FE-LOS, page 2-67	RFI-P, page 2-102
AS-MT, page 2-24	FE-MANWKSWPR-RING, page 2-67	RFI-V, page 2-102
AUD-LOG-LOSS, page 2-24	FE-MANWKSWPR-SPAN, page 2-68	RING-SW-EAST, page 2-104
AUD-LOG-LOW, page 2-25	FORCED-REQ, page 2-69	RING-SW-WEST, page 2-104
AUTOSW-AIS, page 2-25	FORCED-REQ-RING, page 2-69	SD, page 2-104
AUTOSW-LOP (STSMON), page 2-26	FORCED-REQ-SPAN, page 2-70	SD-L, page 2-105
AUTOSW-PDI, page 2-26	FRCDSWTOINT, page 2-70	SD-P, page 2-106
AUTOSW-SDBER, page 2-27	FRCDSWTOPRI, page 2-70	SF, page 2-106
AUTOSW-SFBER, page 2-27	FRCDSWTOSEC, page 2-70	SF-L, page 2-107
AUTOSW-UNEQ (STSMON), page 2-27	FRCDSWTOTHIRD, page 2-71	SF-P, page 2-107
BAT-A-HGH-VLT, page 2-28	FRNGSYNC, page 2-71	SPAN-SW-EAST, page 2-108
BAT-A-LOW-VLT, page 2-29	FULLPASSTHR-BI, page 2-72	SPAN-SW-WEST, page 2-109
BAT-B-HGH-VLT, page 2-29	HLDOVRSYNC, page 2-73	SQUELCH, page 2-109
BAT-B-LOW-VLT, page 2-29	INC-ISD, page 2-75	SSM-DUS, page 2-110
CLDRESTART, page 2-36	INHSWPR, page 2-75	SSM-LNC, page 2-111
DS3-MISM, page 2-46	INHSWWKG, page 2-75	SSM-OFF, page 2-111
EXERCISE-RING-REQ, page 2-53	KB-PASSTHR, page 2-76	SSM-PRC, page 2-111
EXERCISE-SPAN-REQ, page 2-53	LKOUTPR-S, page 2-76	SSM-PRS, page 2-111
FAILTOSW, page 2-54	LOCKOUT-REQ, page 2-76	SSM-RES, page 2-112
FAILTOSW-PATH, page 2-55	LOCKOUT-REQ-RING, page 2-77	SSM-SMC, page 2-112
FAILTOSWR, page 2-56	LPBKCRS, page 2-85	SSM-ST2, page 2-112
FAILTOSWS, page 2-58	LPBKFACILITY (DS-N), page 2-86	SSM-ST3, page 2-112

Table 2-4 Conditions Index (continued)

FE-AIS, page 2-60	LPBKFACILITY (OC-N), page 2-87	SSM-ST3E, page 2-113
FE-DS1-MULTLOS, page 2-61	LPBKTERMINAL (DS-N, OC-N), page 2-87	SSM-ST4, page 2-113
FE-DS1-NSA, page 2-61	LPBKTERMINAL (G-Series), page 2-87	SSM-STU, page 2-113
FE-DS1-SA, page 2-62	MAN-REQ, page 2-88	SSM-TNC, page 2-113
FE-DS1-SNGLLOS, page 2-62	MANRESET, page 2-88	SWTOPRI, page 2-115
FE-DS3-NSA, page 2-63	MANSWTOINT, page 2-88	SWTOSEC, page 2-115
FE-DS3-SA, page 2-63	MANSWTOPRI, page 2-89	SWTOTHIRD, page 2-116
FE-EQPT-NSA, page 2-64	MANSWTOSEC, page 2-89	SYNC-FREQ, page 2-116
FE-EXERCISING-RING, page 2-64	MANSWTOTHIRD, page 2-89	WKSWPR, page 2-124
FE-EXERCISING-SPAN, page 2-64	MANUAL-REQ-RING, page 2-89	WTR, page 2-124
FE-FRCDWKSWPR-RING, page 2-65		

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 2-16	FE-DS1-MULTLOS, page 2-61	MEM-GONE, page 2-91
AIS-L, page 2-16	FE-DS1-NSA, page 2-61	MEM-LOW, page 2-92
AIS-P, page 2-17	FE-DS1-SA, page 2-62	MFGMEM, page 2-92
AIS-V, page 2-17	FE-DS1-SNGLLOS, page 2-62	NOT-AUTHENTICATED, page 2-92
APSB, page 2-18	FE-DS3-NSA, page 2-63	PDI-P, page 2-93
APSCDFLTK, page 2-19	FE-DS3-SA, page 2-63	PEER-NORESPONSE, page 2-94
APSC-IMP, page 2-20	FE-EQPT-NSA, page 2-64	PLM-P, page 2-95
APSCINCON, page 2-20	FE-EXERCISING-RING, page 2-64	PLM-V, page 2-96
APSCM, page 2-21	FE-EXERCISING-SPAN, page 2-64	PRC-DUPID, page 2-96
APSCNMIS, page 2-21	FE-FRCDWKSWPR-RING, page 2-65	PROTNA, page 2-97
APSMM, page 2-22	FE-FRCDWKSWPR-SPAN, page 2-65	PWR-A, page 2-98
AS-CMD, page 2-23	FE-IDLE, page 2-66	PWR-B, page 2-99
AS-MT, page 2-24	FE-LOCKOUTOFPR-SPAN, page 2-66	PWR-REDUN, page 2-100
AUD-LOG-LOSS, page 2-24	FE-LOF, page 2-67	RAI, page 2-100
AUD-LOG-LOW, page 2-25	FE-LOS, page 2-67	RCVR-MISS, page 2-101
AUTORESET, page 2-25	FE-MANWKSWPR-RING, page 2-67	RFI-L, page 2-101
AUTOSW-AIS, page 2-25	FE-MANWKSWPR-SPAN, page 2-68	RFI-P, page 2-102
AUTOSW-LOP (STSMON), page 2-26	FEPRLF, page 2-68	RFI-V, page 2-102

Table 2-5 Alphabetical Alarm Index (continued)

AUTOSW-LOP (VTMON), page 2-26	FORCED-REQ, page 2-69	RING-MISMATCH, page 2-103
AUTOSW-PDI, page 2-26	FORCED-REQ-RING, page 2-69	RING-SW-EAST, page 2-104
AUTOSW-SDBER, page 2-27	FORCED-REQ-SPAN, page 2-70	RING-SW-WEST, page 2-104
AUTOSW-SFBER, page 2-27	FRCDSWTOINT, page 2-70	SD, page 2-104
AUTOSW-UNEQ (STSMON), page 2-27	FRCDSWTOPRI, page 2-70	SD-L, page 2-105
AUTOSW-UNEQ (VTMON), page 2-28	FRCDSWTOSEC, page 2-70	SD-P, page 2-106
BAT-A-HGH-VLT, page 2-28	FRCDSWTOTHIRD, page 2-71	SF, page 2-106
BAT-A-LOW-VLT, page 2-29	FRNGSYNC, page 2-71	SF-L, page 2-107
BAT-B-HGH-VLT, page 2-29	FSTSYNC, page 2-71	SF-P, page 2-107
BAT-B-LOW-VLT, page 2-29	FULLPASSTHR-BI, page 2-72	SFTWDOWN, page 2-107
BKUPMEMP, page 2-30	HITEMP, page 2-72	SNTP-HOST, page 2-108
BLSROSYNC, page 2-30	HLDOVRSYNC, page 2-73	SPAN-SW-EAST, page 2-108
CARLOSS (EQPT), page 2-31	IMPROPRMVL, page 2-73	SPAN-SW-WEST, page 2-109
CARLOSS (E Series), page 2-32	INC-ISD, page 2-75	SQUELCH, page 2-109
CARLOSS (G Series), page 2-34	INHSWPR, page 2-75	SSM-DUS, page 2-110
CLDRESTART, page 2-36	INHSWWKG, page 2-75	SSM-FAIL, page 2-110
COMIOXC, page 2-37	INVMACADR, page 2-76	SSM-LNC, page 2-111
CONTBUS-A-18, page 2-37	KB-PASSTHR, page 2-76	SSM-OFF, page 2-111
CONTBUS-B-18, page 2-38	LKOUTPR-S, page 2-76	SSM-PRC, page 2-111
CONTBUS-IO-A, page 2-39	LOCKOUT-REQ, page 2-76	SSM-PRS, page 2-111
CONTBUS-IO-B, page 2-40	LOCKOUT-REQ-RING, page 2-77	SSM-RES, page 2-112
CTNEQPT-PBPROT, page 2-41	LOF (BITS), page 2-77	SSM-SMC, page 2-112
CTNEQPT-PBWORK, page 2-43	LOF (DS-1), page 2-78	SSM-ST2, page 2-112
DATAFLT, page 2-45	LOF (DS-3), page 2-79	SSM-ST3, page 2-112
DBOSYNC, page 2-45	LOF (OC-N), page 2-79	SSM-ST3E, page 2-113
DS3-MISM, page 2-46	LOP-P, page 2-80	SSM-ST4, page 2-113
EHIBATVG-A, page 2-46	LOP-V, page 2-81	SSM-STU, page 2-113
EHIBATVG-B, page 2-47	LOS (BITS), page 2-81	SSM-TNC, page 2-113
ELWBATVG-A, page 2-47	LOS (DS-1), page 2-82	SWMTXMOD, page 2-114
ELWBATVG-B, page 2-47	LOS (DS-3), page 2-83	SWTOPRI, page 2-115
EOC, page 2-48	LOS (OC-N), page 2-84	SWTOSEC, page 2-115
EQPT, page 2-50	LPBKCRS, page 2-85	SWTOTHIRD, page 2-116
EQPT-MISS, page 2-51	LPBKFACILITY (DS-N), page 2-86	SYNC-FREQ, page 2-116
E-W-MISMATCH, page 2-51	LPBKFACILITY (OC-N), page 2-87	SYNCPRI, page 2-117
EXCCOL, page 2-53	LPBKTERMINAL (DS-N, OC-N), page 2-87	SYNCSEC, page 2-117

Table 2-5 Alphabetical Alarm Index (continued)

EXERCISE-RING-REQ, page 2-53	LPBKTERMINAL (G-Series), page 2-87	SYNCTHIRD, page 2-118
EXERCISE-SPAN-REQ, page 2-53	MAN-REQ, page 2-88	SYSBOOT, page 2-119
EXT, page 2-54	MANRESET, page 2-88	TIM-P, page 2-119
EXTRA-TRAF-PREEMPT, page 2-54	MANSWTOINT, page 2-88	TPTFAIL (G-Series), page 2-120
FAILTOSW, page 2-54	MANSWTOPRI, page 2-89	TRMT, page 2-121
FAILTOSW-PATH, page 2-55	MANSWTOSEC, page 2-89	TRMT-MISS, page 2-121
FAILTOSWR, page 2-56	MANSWTOTHIRD, page 2-89	UNEQ-P, page 2-122
FAILTOSWS, page 2-58	MANUAL-REQ-RING, page 2-89	UNEQ-V, page 2-124
FAN, page 2-59	MANUAL-REQ-SPAN, page 2-90	WKSWPR, page 2-124
FANDEGRADE, page 2-60	MEA (EQPT), page 2-90	WTR, page 2-124
FE-AIS, page 2-60		

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

BITS:: LOS (BITS), page 2-81
BITS:: AIS, page 2-16
BITS:: LOF (BITS), page 2-77
BITS:: SSM-DUS, page 2-110
BITS:: SSM-FAIL, page 2-110
BITS:: SSM-OFF, page 2-111
BITS:: SSM-PRS, page 2-111
BITS:: SSM-RES, page 2-112
BITS:: SSM-SMC, page 2-112
BITS:: SSM-ST2, page 2-112
BITS:: SSM-ST3, page 2-112
BITS:: SSM-ST3E, page 2-113
BITS:: SSM-ST4, page 2-113
BITS:: SSM-STU, page 2-113
BITS:: SSM-TNC, page 2-113
DS1:: AIS, page 2-16
DS1:: AS-CMD, page 2-23
DS1:: AS-MT, page 2-24
DS1:: LOF (DS-1), page 2-78

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

DS1:: LOS (DS-1), page 2-82
DS1:: LPBKFACILITY (DS-N), page 2-86
DS1:: LPBKTERMINAL (DS-N, OC-N), page 2-87
DS1:: RAI, page 2-100
DS1:: RCVR-MISS, page 2-101
DS3:: SD, page 2-104
DS3:: SF, page 2-106
DS1:: TRMT, page 2-121
DS1:: TRMT-MISS, page 2-121
DS3:: AIS, page 2-16
DS3:: AS-CMD, page 2-23
DS3:: AS-MT, page 2-24
DS3:: DS3-MISM, page 2-46
DS3:: FE-AIS, page 2-60
DS3:: FE-DS1-MULTLOS, page 2-61
DS3:: FE-DS1-NSA, page 2-61
DS3:: FE-DS1-SA, page 2-62
DS3:: FE-DS1-SNGLLOS, page 2-62
DS3:: FE-DS3-NSA, page 2-63
DS3:: FE-DS3-SA, page 2-63
DS3:: FE-EQPT-NSA, page 2-64
DS3:: FE-IDLE, page 2-66
DS3:: FE-LOF, page 2-67
DS3:: FE-LOS, page 2-67
DS3:: INC-ISD, page 2-75
DS3:: LOF (DS-3), page 2-79
DS3:: LOS (DS-3), page 2-83
DS3:: LPBKFACILITY (DS-N), page 2-86
DS3:: LPBKTERMINAL (DS-N, OC-N), page 2-87
DS3:: RAI, page 2-100
ENV:: EXT, page 2-54
EQPT:: AS-CMD, page 2-23
EQPT:: AUTORESET, page 2-25
EQPT:: BKUPMEMP, page 2-30
EQPT:: CARLOSS (EQPT), page 2-31
EQPT:: CLDRESTART, page 2-36
EQPT:: COMIOXC, page 2-37

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

EQPT:: CONTBUS-A-18, page 2-37
EQPT:: CONTBUS-B-18, page 2-38
EQPT:: CONTBUS-IO-A, page 2-39
EQPT:: CONTBUS-IO-B, page 2-40
EQPT:: CTNEQPT-PBPROT, page 2-41
EQPT:: CTNEQPT-PBWORK, page 2-43
EQPT:: EQPT, page 2-50
EQPT:: EXCCOL, page 2-53
EQPT:: FAILTOSW, page 2-54
EQPT:: FORCED-REQ, page 2-69
EQPT:: HITEMP, page 2-72
EQPT:: IMPROPRMVL, page 2-73
EQPT:: INHSWPR, page 2-75
EQPT:: INHSWWKG, page 2-75
EQPT:: LOCKOUT-REQ, page 2-76
EQPT:: MAN-REQ, page 2-88
EQPT:: MANRESET, page 2-88
EQPT:: MEA (EQPT), page 2-90
EQPT:: MEM-GONE, page 2-91
EQPT:: MEM-LOW, page 2-92
EQPT::PEER-NORESPONSE, page 2-94
EQPT:: PROTNA, page 2-97
EQPT:: PWR-REDUN, page 2-100
EQPT:: SD, page 2-104
EQPT:: SFTWDOWN, page 2-107
EQPT:: SWMTXMOD, page 2-114
EQPT:: WKSWPR, page 2-124
EQPT:: WTR, page 2-124
ETHER:: AS-CMD, page 2-23
ETHER:: CARLOSS (E Series), page 2-32
ETHER:: CARLOSS (G Series), page 2-34
EXTSYNCH:: FRCDSWTOPRI, page 2-70
EXTSYNCH:: FRCDSWTOSEC, page 2-70
EXTSYNCH:: FRCDSWTOTHIRD, page 2-71
EXTSYNCH:: MANSWTOPRI, page 2-89
EXTSYNCH:: MANSWTOSEC, page 2-89
EXTSYNCH:: MANSWTOTHIRD, page 2-89

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

EXTSYNCH:: SWTOPRI, page 2-115
EXTSYNCH:: SWTOSEC, page 2-115
EXTSYNCH:: SWTOTHIRD, page 2-116
EXTSYNCH:: SYNCPRI, page 2-117
EXTSYNCH:: SYNCSEC, page 2-117
EXTSYNCH:: SYNCTHIRD, page 2-118
FAN:: EQPT-MISS, page 2-51
FAN:: FAN, page 2-59
FAN:: FANDEGRADE, page 2-60
FAN:: MEM-GONE, page 2-91
FAN:: MFGMEM, page 2-92
HDGE [G1000]:: AS-CMD, page 2-23
HDGE [G1000]:: AS-MT, page 2-24
HDGE [G1000]:: CARLOSS (G Series), page 2-34
HDGE [G1000]:: LPBKTERMINAL (G-Series), page 2-87
HDGE [G1000]:: TPTFAIL (G-Series), page 2-120
NBR:: SD, page 2-104
NE:: AS-CMD, page 2-23
NE:: AUD-LOG-LOSS, page 2-24
NE:: AUD-LOG-LOW, page 2-25
NE:: BAT-A-HGH-VLT, page 2-28
NE:: BAT-A-LOW-VLT, page 2-29
NE:: BAT-B-HGH-VLT, page 2-29
NE:: BAT-B-LOW-VLT, page 2-29
NE:: DATAFLT, page 2-45
NE:: DBOSYNC, page 2-45
NE:: EHIBATVG-A, page 2-46
NE:: EHIBATVG-B, page 2-47
NE:: ELWBATVG-A, page 2-47
NE:: ELWBATVG-B, page 2-47
NE:: HITEMP, page 2-72
NE:: PRC-DUPID, page 2-96
NE:: PWR-A, page 2-98
NE:: PWR-B, page 2-99
NE:: SNTP-HOST, page 2-108
NE:: SYSBOOT, page 2-119
NERING:: BLSROSYNC, page 2-30

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

NERING:: FULLPASSTHR-BI, page 2-72
NERING:: KB-PASSTHR, page 2-76
NERING:: PRC-DUPID, page 2-96
NERING:: RING-MISMATCH, page 2-103
NESYNCH:: FRCDSWTOINT, page 2-70
NESYNCH:: FRCDSWTOPRI, page 2-70
NESYNCH:: FRCDSWTOSEC, page 2-70
NESYNCH:: FRCDSWTOTHIRD, page 2-71
NESYNCH:: FRNGSYNC, page 2-71
NESYNCH:: FSTSYNC, page 2-71
NESYNCH:: HLDOVRSYNC, page 2-73
NESYNCH:: MANSWTOINT, page 2-88
NESYNCH:: MANSWTOPRI, page 2-89
NESYNCH:: MANSWTOSEC, page 2-89
NESYNCH:: MANSWTOTHIRD, page 2-89
NESYNCH:: SSM-PRS, page 2-111
NESYNCH:: SSM-RES, page 2-112
NESYNCH:: SSM-SMC, page 2-112
NESYNCH:: SSM-ST2, page 2-112
NESYNCH:: SSM-ST3, page 2-112
NESYNCH:: SSM-ST3E, page 2-113
NESYNCH:: SSM-ST4, page 2-113
NESYNCH:: SSM-STU, page 2-113
NESYNCH:: SSM-TNC, page 2-113
NESYNCH:: SWTOPRI, page 2-115
NESYNCH:: SWTOSEC, page 2-115
NESYNCH:: SWTOTHIRD, page 2-116
NESYNCH:: SYNCPRI, page 2-117
NESYNCH:: SYNCSEC, page 2-117
NESYNCH:: SYNCTHIRD, page 2-118
OCN:: AIS-L, page 2-16
OCN:: APSB, page 2-18
OCN:: APSCDFLTK, page 2-19
OCN:: APSC-IMP, page 2-20
OCN:: APSCINCON, page 2-20
OCN:: APSCM, page 2-21
OCN:: APSCNMIS, page 2-21

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

OCN:: APSMM, page 2-22
OCN:: AS-CMD, page 2-23
OCN:: AS-MT, page 2-24
OCN:: EOC, page 2-48
OCN:: E-W-MISMATCH, page 2-51
OCN:: EXERCISE-RING-REQ, page 2-53
OCN:: EXERCISE-SPAN-REQ, page 2-53
OCN:: EXTRA-TRAF-PREEMPT, page 2-54
OCN:: FAILTOSW, page 2-54
OCN:: FAILTOSWR, page 2-56
OCN:: FAILTOSWS, page 2-58
OCN:: FE-EXERCISING-RING, page 2-64
OCN:: FE-EXERCISING-SPAN, page 2-64
OCN:: FE-FRCDWKSWPR-RING, page 2-65
OCN:: FE-FRCDWKSWPR-SPAN, page 2-65
OCN:: FE-LOCKOUTOFPR-SPAN, page 2-66
OCN:: FE-MANWKSWPR-RING, page 2-67
OCN:: FE-MANWKSWPR-SPAN, page 2-68
OCN:: FEPRLF, page 2-68
OCN:: FORCED-REQ-RING, page 2-69
OCN:: FORCED-REQ-SPAN, page 2-70
OCN:: LKOUTPR-S, page 2-76
OCN:: LOCKOUT-REQ, page 2-76
OCN:: LOCKOUT-REQ-RING, page 2-77
OCN:: LOF (OC-N), page 2-79
OCN:: LOS (OC-N), page 2-84
OCN:: LPBKFACILITY (OC-N), page 2-87
OCN:: LPBKTERMINAL (DS-N, OC-N), page 2-87
OCN:: MANUAL-REQ-RING, page 2-89
OCN:: MANUAL-REQ-SPAN, page 2-90
OCN:: RFI-L, page 2-101
OCN:: RING-SW-EAST, page 2-104
OCN:: RING-SW-WEST, page 2-104
OCN:: SD-L, page 2-105
OCN:: SF-L, page 2-107
OCN:: SPAN-SW-EAST, page 2-108
OCN:: SPAN-SW-WEST, page 2-109

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

OCN:: SQUELCH, page 2-109
OCN:: SSM-DUS, page 2-110
OCN:: SSM-FAIL, page 2-110
OCN:: SSM-OFF, page 2-111
OCN:: SSM-PRS, page 2-111
OCN:: SSM-RES, page 2-112
OCN:: SSM-SMC, page 2-112
OCN:: SSM-ST2, page 2-112
OCN:: SSM-ST3, page 2-112
OCN:: SSM-ST3E, page 2-113
OCN:: SSM-ST4, page 2-113
OCN:: SSM-STU, page 2-113
OCN:: SSM-TNC, page 2-113
OCN:: SYNC-FREQ, page 2-116
OCN:: WKSWPR, page 2-124
OCN:: WTR, page 2-124
STSMON:: AIS-P, page 2-17
STSMON:: AUTOSW-AIS, page 2-25
STSMON:: AUTOSW-LOP (STSMON), page 2-26
STSMON:: AUTOSW-PDI, page 2-26
STSMON:: AUTOSW-SDBER, page 2-27
STSMON:: AUTOSW-SFBER, page 2-27
STSMON:: AUTOSW-UNEQ (STSMON), page 2-27
STSMON:: FAILTOSW-PATH, page 2-55
STSMON:: FORCED-REQ, page 2-69
STSMON:: LOCKOUT-REQ, page 2-76
STSMON:: LOP-P, page 2-80
STSMON:: LPBKCRS, page 2-85
STSMON:: MAN-REQ, page 2-88
STSMON:: PDI-P, page 2-93
STSMON:: PLM-P, page 2-95
STSMON:: RFI-P, page 2-102
STSMON:: SD-P, page 2-106
STSMON:: SF-P, page 2-107
STSMON:: TIM-P, page 2-119
STSMON:: UNEQ-P, page 2-122
STSMON:: WKSWPR, page 2-124

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

STSMON:: WTR, page 2-124
STSTERM:: AIS-P, page 2-17
STSTERM:: LOP-P, page 2-80
STSTERM:: PDI-P, page 2-93
STSTERM:: PLM-P, page 2-95
STSTERM:: RFI-P, page 2-102
STSTERM:: SD-P, page 2-106
STSTERM:: SF-P, page 2-107
STSTERM:: TIM-P, page 2-119
STSTERM:: UNEQ-P, page 2-122
VT-MON:: AIS-V, page 2-17
VT-MON:: AUTOSW-AIS, page 2-25
VT-MON:: AUTOSW-LOP (VTMON), page 2-26
VT-MON:: AUTOSW-UNEQ (VTMON), page 2-28
VT-MON:: FAILTOSW-PATH, page 2-55
VT-MON:: FORCED-REQ, page 2-69
VT-MON:: LOCKOUT-REQ, page 2-76
VT-MON:: LOP-V, page 2-81
VT-MON:: MAN-REQ, page 2-88
VT-MON:: UNEQ-V, page 2-124
VT-MON:: WKSWPR, page 2-124
VT-MON:: WTR, page 2-124
VT-TERM:: AIS-V, page 2-17
VT-TERM:: PLM-V, page 2-96
VT-TERM:: RFI-V, page 2-102
VT-TERM:: SD-P, page 2-106
VT-TERM:: SF-P, page 2-107
VT-TERM:: UNEQ-V, page 2-124

2.3.1 Alarm Type/Object Definition

Table 2-7 defines abbreviations used in the alarm troubleshooting procedures.

Table 2-7 Alarm Type/Object Definition

BITS	Building integration timing supply (BITS) incoming references (BITS-1, BITS-2)
DS1	A DS-1 line on an XTC-14 or XTC-28-3 card
DS3	A DS-3 line on an XTC-28-3 card

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

ENV	An environmental alarm port on an XTC card
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 (Category 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 G1000-2 cards.
MSUDC	SONET Multiplex Section User Data Channel
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 OCN 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 15327 uses standard Telcordia categories to characterize levels of trouble. The ONS 15327 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) alarm (see page 2-84). Conditions notify the user of an event which does not require action, such as a SWTOSEC condition (see page 2-115) or a MANRESET condition (see page 2-88).

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-MISS alarm (see page 2-121) is characterized as an SA failure. TRMT-MISS occurs when the cable connector leading to a DS-1 port on an XTC card is removed. This affects a provided service because traffic switches to the protect card. The HITEMP alarm (see page 2-72) 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 15327 also sends an AIS condition (see page 2-16) downstream. When the node receives the AIS, the node sends an RFI-L condition (see page 2-101) upstream. AIS 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 15327 uses Telcordia 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-48 card, a Critical alarm, approximately 25,000 DS-0 circuits lose protection.

Minor alarms, such as the FSTSYNC alarm (see page 2-71), do not have a serious affect on service. FSTSYNC lets you know that the ONS 15327 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 15327. A user may customize ONS 15327 alarm severities with the alarm profiles feature. For alarm profile procedures, refer to the *Cisco ONS 15327 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 15327. 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 when the system is operating. Use caution when removing or installing cards.

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 are 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 15327 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.

Clear the AIS Condition

Step 1 Verify whether there are alarms on the upstream nodes and equipment, especially an LOS (OC-N) alarm (see page 2-84) 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 (AIS-L) 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-L, 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) alarm (see page 2-84) 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.

Clear the AIS-L Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-16.

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 (AIS-P) 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-P 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) alarm (see page 2-84) or has an OC-N port OOS. 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.

Clear the AIS-P Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-16.

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-V, 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) alarm (see page 2-84) or has an 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 condition (see page 2-17) on the cross connected OC-N card.

Note If the AIS-V occurred on an XTC-28-3 unused circuit, complete the "Clear AIS-V on XTC-28-3 Unused VT Circuits" procedure on page 1-67.

Clear the AIS-V Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-16.

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 (APSB) 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 15327. These invalid codes causes an APSB on an ONS node.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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 15327.

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.

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

Troubleshooting for APSCDFLTK is often similar to troubleshooting for a BLSROSYNC alarm (see page 2-30).

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the APSCDFLTK Alarm

Step 1 Complete the "Identify a Ring ID or Node ID Number" procedure on page 2-126 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 2-126 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 2-51.) West port fibers must connect to east port fibers, and vice versa. The *Cisco ONS 15327 Procedure Guide* provides a procedure for fibering BLSRs.

Step 5 If the alarm does not clear and if the network is a 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 2-126.

Step 7 If nodes are not visible, complete the "Verify or Create Node DCC Terminations" procedure on page 2-127 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 (APSC-IMP) 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.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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 15327. Troubleshoot the upstream equipment using the procedures in this chapter, as applicable. If the upstream nodes are not ONS 15327s, 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 2-126.

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 2-126.

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 (APSCINCON) alarm means that an inconsistent APS byte is present. The SONET overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15327, to switch the SONET signal from a working to a protect path. An inconsistent APS code occurs when three consecutive frames do not contain identical APS bytes. Inconsistent APS bytes give the receiving equipment conflicting commands about switching.

Clear the APSCINCON Alarm

Step 1 Look for other alarms, especially an LOS (OC-N) alarm (see page 2-84), an LOF (OC-N) alarm (see page 2-79), or an AIS condition (see page 2-16). 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 (APSCM) alarm occurs when the ONS 15327 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 15327 when bidirectional protection is used on OC-N cards in a 1+1 configuration.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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 (APSCNMIS) 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.

Clear the APSCNMIS Alarm

Step 1 Complete the "Identify a Ring ID or Node ID Number" procedure on page 2-126 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 2-126 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 15327 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 2-127 to lock out the span.

Step 6 Complete the "Clear a BLSR Span Lock Out" procedure on page 2-127 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 (APSMM) alarm occurs when there is a mismatch of the protection switching schemes at the two ends of the span. If one node is provisioned for bidirectional switching, the node at the other end of the span must also be provisioned for bidirectional switching. If one end is provisioned for bidirectional and the other is provisioned for unidirectional, an APSMM alarm occurs in the ONS node that is provisioned for bidirectional. The APSMM alarm occurs in a 1+1 configuration.

Clear the APSMM Alarm

Step 1 For the reporting ONS 15327, 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 (AS-CMD) condition applies to the network element (NE, or node) and cards. It occurs when alarms are suppressed for one or more cards or for the entire shelf.

Clear the AS-CMD Condition

Step 1 In node view, click the **Conditions** tab.

Step 2 Click **Retrieve**. If you have already retrieved conditions, look under the Object column and Eqpt Type column, and note what entity the condition is reported against, such as a port, slot, or shelf.

If the condition is reported against a slot and card, alarms were either suppressed for the entire card or for one of the ports. Note the slot number and continue with Step 3.

If the Condition window says that the object is "system," the condition applies to the shelf. Go to Step 7.

Step 3 If the AS-CMD condition is reported for a card, determine if 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 the check box 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 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 8 If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.13 AS-MT

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

The Alarms Suppressed for Maintenance Command (AS-MT) 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.

Clear the AS-MT Condition

Step 1 Complete the "Clear a Loopback" procedure on page 2-129.

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 (AUD-LOG-LOS) condition occurs when the log is 100 percent full and that the oldest entries are being replaced as new entries are generated. The log capacity is 640 entries.

Clear the AUD-LOG-LOSS Condition

Step 1 In node view, click the **Maintenance > Audit** tabs.

Step 2 Click **Retrieve**.

Step 3 Click **Archive**.

Step 4 In the Archive Audit Trail dialog box, navigate to the directory (local or network) where you want to save the file.

Step 5 Enter a name in the File name field.

You do not have to assign an extension to the file. It is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.

Step 6 Click **Save**.

The 640 entries will be saved in this file. New entries will continue with the next number in the sequence, rather than starting over.

Step 7 If the alarm does not clear, log onto http://www.cisco.com/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 Low (AUD-LOG-LOW) condition occurs when the audit trail log is 80 percent full.

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

2.6.16 AUTORESET

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

The Automatic System Reset (AUTORESET) alarm occurs when you change an IP address or perform any other operation that causes an automatic card-level reboot. This alarm typically clears after a card reboots (up to ten minutes). If the alarm does not clear, complete the following procedure.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the AUTORESET Alarm

Step 1 Look for any 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 2-130.

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

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).

2.6.17 AUTOSW-AIS

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

The AutomaticPath Protection Switch Caused by AIS (AUTOSW-AIS) condition indicates that automatic path protection switching occurred because of an AIS condition. If the path protection is configured for revertive switching, it will revert to the working path after the fault clears.

Clear the AUTOSW-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-16.

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).

2.6.18 AUTOSW-LOP (STSMON)

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

The Automatic Path Protection Switch Caused by Loss of Pointer (LOP) condition indicates that automatic path protection switching occurred because of an LOP-P alarm (see page 2-80). If the path protection is configured for revertive switching, it will revert to the working path after the fault clears.

Clear the AUTOSW-LOP (STSMON) Condition

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-81.

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 (VTMON)

- Minor (MN), Service Affecting (SA)

The AUTOSW-LOP alarm indicates that automatic path protection switching occurred because of an LOP-V alarm (see page 2-81). If the path protection is configured for revertive switching, it will revert to the working path after the fault clears.

Clear the AUTOSW-LOP (VTMON) Alarm

Step 1 Complete the "Clear the LOP-V Alarm" procedure on page 2-81.

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).

2.6.20 AUTOSW-PDI

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

The Automatic Path Protection Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic path protection switching occurred because of a PDI-P alarm (see page 2-93). If the path protection is configured for revertive switching, it will revert to the working path after the fault clears.

Clear the AUTOSW-PDI Condition

Step 1 Complete the "Clear the PDI-P Condition" procedure on page 2-93.

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).

2.6.21 AUTOSW-SDBER

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

The Automatic Path Protection Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that an SD condition (see page 2-104) caused automatic path protection protection switching to occur. The path protection is configured for revertive switching and reverts to the working path when the SD is resolved.

Clear the AUTOSW-SDBER Condition

Step 1 Complete the "Clear the SD Condition" 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 (1-800-553-2447).

2.6.22 AUTOSW-SFBER

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

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that an SF condition (see page 2-106) condition caused automatic path protection switching to occur. The path protection is configured for revertive switching and reverts to the working path when the SF is resolved.

Clear the AUTOSW-SFBER Condition

Step 1 Complete the "Clear the SF Condition" procedure on page 2-106.

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-UNEQ (STSMON)

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

The Automatic Path Protection Switch Caused by an UNEQ-P alarm (see page 2-122) indicates that an UNEQ alarm caused automatic path protection protection switching to occur. If the path protection is configured for revertive switching, it will revert to the working path after the fault clears.

Clear the AUTOSW-UNEQ (STSMON) Condition

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-123.

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).

2.6.24 AUTOSW-UNEQ (VTMON)

- Minor (MN), Service Affecting (SA)

AUTOSW-UNEQ (VTMON) indicates that an UNEQ-V alarm (see page 2-124) caused automatic path protection switching to occur. If the path protection is configured for revertive switching, it will revert to the working path after the fault clears.

Clear the AUTOSW-UNEQ (VTMON) Alarm

Step 1 Complete the "Clear the UNEQ-V Alarm" procedure on page 2-124.

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).

2.6.25 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.

Clear the BAT-A-HGH-VLT Condition

Step 1 The problem is external to the ONS 15327. 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).

2.6.26 BAT-A-LOW-VLT

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

The Low Voltage Battery A (BAT-A-LOW-VLT) 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.

Clear the BAT-A-LOW-VLT Condition

Step 1 The problem is external to the ONS 15327. 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-B-HGH-VLT

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

The High Voltage Battery B (BAT-B-HGH-VLT) 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.

Clear the BAT-B-HGH-VLT Condition

Step 1 The problem is external to the ONS 15327. 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).

2.6.28 BAT-B-LOW-VLT

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

The Low Voltage Battery B (BAT-B-LOW-VLT) 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.

Clear the BAT-B-LOW-VLT Condition

Step 1 The problem is external to the ONS 15327. 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 BKUPMEMP

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

The Primary Non-Volatile Backup Memory Failure (BKUPMEMP) alarm refers to a problem with the XTC card's Flash memory. The alarm occurs when the XTC 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 the cyclic redundancy check (CRC). CRC is a method to verify for errors in data transmitted to the XTC.

The BKUPMEMP alarm can also cause the EQPT alarm (see page 2-50). 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 XTC card.

Clear the BKUPMEMP Alarm

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

Step 2 If both XTC cards are powered and enabled, reset the active XTC card to it standby and make the standby XTC card active. Complete the "Reset the Active XTC Card in CTC" procedure on page 2-129.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

Step 3 If the XTC 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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.30 BLSROSYNC

- Major (MJ), Service Affecting (SA)

The BLSR Out Of Synchronization (BLSROSYNC) 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.

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.**

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 2-48.

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).

2.6.31 CARLOSS (EQPT)

- Major (MJ), Service Affecting (SA)

A Carrier Loss on the LAN Equipment (CARLOSS) alarm occurs when the ONS 15327 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 XTC card. 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 15327.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the CARLOSS (EQPT) Alarm

Step 1 Verify connectivity by pinging the ONS 15327 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 15327 IP address]
```

For example, ping 192.1.0.2.

If the workstation has connectivity to the ONS 15327, 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 (Category 5) LAN cable is properly connected and attached to the correct port.

Step 4 If the straight-through (Category 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 cable 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).

2.6.32 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) alarm (see page 2-84). 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 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 G1000-2 card, because the G1000-2 card does not use STP and is unaffected by STP reestablishment.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the CARLOSS (E-Series) Alarm

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

Step 2 If the straight-through (Category 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 (Category 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 2-130 for the Ethernet (traffic) card.

Step 7 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the Ethernet (traffic) card.

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 15327 and card host the Ethernet circuit at the other end of the Ethernet manual cross-connect:

- Log into the ONS 15327 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. Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size.

f. If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-128 and reconfigure the circuit with the correct circuit size. For more information, refer to the *Cisco ONS 15327 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).

2.6.33 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) alarm (see page 2-84). The Ethernet card has lost its link and is not receiving a valid signal.

CARLOSS on the G1000-2 card is caused by one of two situations:

- The G1000-2 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 G1000-2 port.
- If a problem exists in the end-to-end path (including possibly the far-end G1000-2 card), it causes the reporting G1000-2 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 G1000-2 card. The root cause is the problem in the end-to-end path. When the root cause is cleared, the far-end G1000-2 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 a TPTFAIL (G-Series) alarm (see page 2-120) or OC-N alarms or conditions on the end-to-end path normally accompany the CARLOSS (G-Series) alarm.

Refer to the *Cisco ONS 15327 Reference Manual* for a description of the G1000-2 card's end-to-end Ethernet link integrity capability. Also see the "TRMT" section on page 2-121 for more information about alarms that occur when a point-to-point circuit exists between two G1000-2 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.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the CARLOSS (G Series) Alarm

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

Step 2 If the straight-through (Category 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 (Category 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 G1000-2 port, but the autonegotiation process fails, the G1000-2 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 G1000-2.

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) alarm (see page 2-120) alarm is also reported, complete the "Clear the TPTFAIL (G-Series) Alarm" procedure on page 2-120. 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 G1000-2'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 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 in service (IS) is listed, go to Step 11.

Step 10 If a loopback was provisioned, complete the "Clear a Loopback" procedure on page 2-129.

On the G1000-2 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 G1000-2 card. Terminating the transmit laser could raise the CARLOSS alarm because the loopbacked G1000-2 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 15327s, and the OSI/TARP-based equipment does not allow tunneling of the ONS 15327 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 15327 and card host the Ethernet circuit at the other end of the Ethernet manual cross-connect:

- Log into the ONS 15327 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 (traffic) 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 2-128 and reconfigure the circuit with the correct circuit size. Refer to the *Cisco ONS 15327 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 2-130.

Step 13 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the Ethernet (traffic) card.

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).

2.6.34 CLDRESTART

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

The Cold Restart (CLDRESTART) condition occurs when a card is physically removed and inserted, replaced, or when the ONS 15327 is first powered up.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the CLDRESTART Condition

Step 1 If the condition fails to clear after the card reboots, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130.

Step 2 If you reinsert a high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 3 If the condition does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the card.

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

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).

2.6.35 COMIOXC

- Critical (CR), Service Affecting (SA)

The Input/Output Slot To XTC Communication Failure (COMIOXC) alarm is caused by a communication error in the XTC card to a high-speed traffic card slot.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the COMIOXC Alarm

Step 1 Complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 on the reporting XTC card.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

Step 2 Complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the reporting XTC card.

Step 3 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting XTC card.

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

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).

2.6.36 CONTBUS-A-18

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

A Communication Failure from XTC A Slot to XTC Slot alarm occurs when the main processor on the XTC card in Slot 5(termed XTC A) loses communication with the coprocessor on the same card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the CONTBUS-A-18 Alarm

Step 1 Complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 to make the XTC in Slot 6 active.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

Step 2 Position the cursor over the XTC card in Slot 6 and complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 to make the standby XTC in Slot 5 active.

Step 3 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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.37 CONTBUS-B-18

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

A Communication Failure from XTC Slot to XTC slot alarm occurs when the main processor on the XTC card in Slot 6 (termed XTC B) loses communication with the coprocessor on the same card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the CONTBUS-B-18 Alarm

Step 1 Position the cursor over the XTC card in Slot 6 and complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 to make the XTC in Slot 5 active.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

Step 2 Position the cursor over the XTC card in Slot 5 and complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 to make the standby XTC in Slot 6 active.

Step 3 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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.38 CONTBUS-IO-A

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

An XTC A to Shelf Slot Communication Failure alarm occurs when the XTC card in Slot 5 (XTC A) has lost communication with another card in the shelf The other card is identified by the Object column in the CTC alarm window..

The CONTBUS-IO-A alarm can appear briefly when the ONS 15327 switches to the standby XTC card. In the case of an XTC protection switch, the alarm clears after the other cards establish communication with the new active XTC card. If the alarm persists, the problem is with the physical path of communication from the XTC to the reporting card. The physical path of communication includes the XTC card, the other card, and the backplane.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the CONTBUS-IO-A Alarm

Step 1 Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA (EQPT)" section on page 2-90.

Step 2 If the alarm object is any single card slot other then the standby XTC card in Slot 6, perform a CTC reset of the card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-130.

Step 3 When you reinsert the high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 4 If the alarm object is the standby XTC in Slot 6, perform a soft reset of this card:

a. Right-click the Slot 6 XTC 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 5 Verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 6 If CONTBUS-IO-A is raised on several cards at once, complete the "Reset the Active XTC Card in CTC" procedure on page 2-129. Verify that the card reboots as the standby card.

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 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, 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) a Card" procedure on page 2-130 for the reporting card.

Step 9 If the reseated card or replaced 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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.39 CONTBUS-IO-B

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

An XTC B to Shelf Slot Communication Failure alarm occurs when the XTC card in Slot 6 (XTC 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 can appear briefly when the ONS 15327 switches to the standby XTC card. In the case of an XTC protection switch, the alarm clears after the other cards establish communication with the new active XTC card. If the alarm persists, the problem is with the physical path of communication from the XTC to the reporting card. The physical path of communication includes the XTC card, the other card, and the backplane.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Procedure: Clear the CONTBUS-IO-B Alarm

Step 1 Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA (EQPT)" section on page 2-90.

Step 2 If the alarm object is any single card slot other then the standby XTC card in Slot 5, perform a CTC reset of the card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-130.

Step 3 When you reinsert the high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 4 If the alarm object is the standby XTC in Slot 5, perform a soft reset of this card:

a. Right-click the Slot 5 XTC 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 5 Verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 6 If CONTBUS-IO-B is raised on several cards at once, complete the "Reset the Active XTC Card in CTC" procedure on page 2-129. Verify that the card reboots as the standby card.

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 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, 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) a Card" procedure on page 2-130 for the reporting card.

Step 9 If the reseated card or replaced 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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.40 CTNEQPT-PBPROT

- Critical (CR), Service Affecting (SA)

The Interconnection Equipment Failure Protect XTC Card Payload Bus (CTNEQPT-PBPROT) alarm indicates a failure of the main payload between the protect XTC card and the reporting traffic card. The XTC card and the reporting card are no longer communicating. The problem exists in the XTC card and the reporting traffic card.

Note If all traffic cards show CTNEQPT-PBPROT alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the standby XTC card. If the reseat fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-130 for the standby XTC card. Do not physically reseat an active XTC card. Reseating the XTC disrupts traffic.

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

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the CTNEQPT-PBPROT Alarm

Step 1 Perform a CTC reset on the standby XTC card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-130. (The procedure is the same for the standby XTC as for the traffic card.)

Resetting the standby XTC card will not make it active. Verify that its LED is amber once the reset is complete.

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

Step 2 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the standby XTC card.

Step 3 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 4 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 2-128. After you move traffic off the active card, or if the reporting card is standby, continue with the following steps.

Step 5 Complete the "Reset a Traffic Card in CTC" procedure on page 2-130 on the reporting card.

Step 6 When you reinsert the high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

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 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, 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) a Card" procedure on page 2-130 for the reporting card.

Step 9 Complete the "Clear an External Switching Command" procedure on page 2-128.

Step 10 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the reporting card.

Step 11 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the standby cross-connect card.

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

Step 12 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting traffic card.

Step 13 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).

2.6.41 CTNEQPT-PBWORK

- Critical (CR), Service Affecting (SA)

The Interconnection Equipment Failure Working XTC Card Payload Bus (CTNEQPT-PBWORK) alarm indicates a failure in the main payload bus between the active XTC card the reporting traffic card. The XTC card and the reporting card are no longer communicating. The problem exists in the XTC card or the reporting traffic card.

Note If all traffic cards show CTNEQPT-PBWORK alarm, complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 for the active XTC card and then complete the "Remove and Reinsert (Reseat) the Standby XTC" procedure on page 3-3. If the reseat fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-130 for the XTC card. Do not physically reseat an active XTC card; it disrupts traffic.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the CTNEQPT-PBWORK Alarm

Step 1 Complete the "Reset the Active XTC Card in CTC" procedure on page 2-129 for the active XTC card.

Caution Resetting the active XTC is traffic-affecting.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

Step 2 Complete the "Reset a Traffic Card in CTC" procedure on page 2-130 for the reporting card.

The reboot takes up to ten minutes.

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 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, 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 2-130 for the standby XTC 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 2-128. 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 2-130 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 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, 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) a Card" procedure on page 2-130 for the reporting card.

Step 9 If you reinsert a high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 10 If you switched traffic, complete the "Clear an External Switching Command" procedure on page 2-128.

Step 11 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the cross-connect card.

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

Step 12 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting traffic card.

Step 13 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).

2.6.42 DATAFLT

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

The Software Data Integrity Fault (DATAFLT) alarm occurs when the XTC exceeds its Flash memory capacity.

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

Clear the DATAFLT Alarm

Step 1 Complete the "Reset the Active XTC Card in CTC" procedure on page 2-129.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

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).

2.6.43 DBOSYNC

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

The Standby Database Out of Synchronization (DBOSYNC) alarm occurs when the standby XTC "To be Active" database does not synchronize with the "Active" database on the active XTC.

Caution If you reset the active XTC while this alarm is raised, you will lose current provisioning.

Clear the DBOSYNC Alarm

Step 1 Save a backup copy of the active XTC database. Complete the "Back Up the Database" procedure in the *Cisco ONS 15327 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 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 does 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).

2.6.44 DS3-MISM

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

The DS-3 Frame Format Mismatch (DS3-MISM) condition indicates a DS-1 frame format mismatch on a signal transiting the XTC-28-3 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 D4 for a DS-1 transiting the XTC-28-3 card, and the incoming signal's line type format is detected as unframed, then the ONS 15327 reports a DS3-MISM condition.

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.**

Note You can only provision DS-1 line frame format on the XTC-28-3 card. DS-3 line format is not provisionable.

Clear the DS3-MISM Condition

Step 1 Display the CTC card view for the reporting (active) XTC-28-3 card.

Step 2 Click the **Provisioning > DS1 > 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 (ESF, D4, or unframed).

Step 4 If the Line Type drop-down menu does not match the expected incoming signal, select the correct Line Type in the drop-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 15327 matches the expected incoming signal.

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

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).

2.6.45 EHIBATVG-A

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

The Extreme High Voltage Battery A (EHIBATVG-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.

Clear the EHIBATVG-A Alarm

Step 1 The problem is external to the ONS 15327. 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).

2.6.46 EHIBATVG-B

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

The Extreme High Voltage Battery B (EHIBATVG-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.

Clear the EHIBATVG-B Alarm

Step 1 The problem is external to the ONS 15327. 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).

2.6.47 ELWBATVG-A

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

The Extreme Low Voltage Battery A (ELWBATVG-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.

Clear the ELWBATVG-A Alarm

Step 1 The problem is external to the ONS 15327. 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).

2.6.48 ELWBATVG-B

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

The Extreme Low Voltage Battery B (ELWBATVG-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.

Clear the ELWBATVG-B Alarm

Step 1 The problem is external to the ONS 15327. 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).

2.6.49 EOC

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

The SONET DCC Termination Failure (EOC) alarm occurs when the ONS 15327 loses its data communications channel. The DCC is three bytes, D1 through D3, in the SONET overhead that convey information about Operation, Administration, Maintenance, and Provisioning (OAM&P). The ONS 15327 uses the DCC on the SONET section layer to communicate network management information.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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.

Clear the EOC Alarm

Step 1 If an LOS (DS-1) alarm (see page 2-82) is also reported, complete the "Clear the LOS (DS-1) Alarm" procedure on page 2-82.

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 2-127 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 in service (IS).
- **e.** If the State column lists the port as OOS, click the column and click **IS** from the drop-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 (traffic) card. It might be necessary to externally 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 1-77.

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 15327 Procedure Guide*.

Step 10 If fiber connectors are properly fastened and terminated, complete the "Reset the Active XTC Card in CTC" procedure on page 2-129.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

If the alarm clears when the ONS 15327 switches to the standby XTC, the user can assume that the original active XTC is the cause of the alarm.

Step 11 If the XTC replacement does not clear the alarm, delete the problematic DCC termination:

- **a.** Click the **Provisioning > SONET DCC** 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 15327 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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.50 EQPT

- Critical (CR), Service Affecting (SA)

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

If the EQPT alarm occurs with a BKUPMEMP alarm, see the "BKUPMEMP" section on page 2-30. The BKUPMEMP procedure also clears the EQPT alarm.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the EQPT Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-130 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 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, 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 2-130.

Step 4 If you reinsert a high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

Step 5 If the physical reseat of the card fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-130.

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

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).

2.6.51 EQPT-MISS

- Critical (CR), Service Affecting (SA)

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

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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 2-131.

Step 3 If no fan-tray assembly is present, obtain a fan-tray assembly and complete the "Install the Fan-Tray Assembly" procedure in the *Cisco ONS 15327 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).

2.6.52 E-W-MISMATCH

- Major (MJ), Service Affecting (SA)

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

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.**

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 1 is west and Slot 4 is east.

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

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

Step 1 Diagram the ring setup, including nodes and spans, on a piece of paper or white board.

Step 2 In node view, click **View > Go to Network View**.

Step 3 Label each of the nodes on the diagram with the same name that appears on the network map.

Step 4 Right-click each span to reveal the node name/slot/port for each end of the span.

Step 5 Label the span ends on the diagram with the same information. For example, with Node1/Slot12/Port1 to 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.

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).

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 2-126 to identify the node ID, ring ID, and the slot and port in the East Line list and West Line columns. Record the 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 drop-down menu to the slot you recorded for the East Line in Step 3.

Step 8 Change the East Line drop-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).

2.6.53 EXCCOL

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

The Excess Collisions on the LAN (EXCCOL) alarm indicates that too many collisions are occurring between data packets on the network management LAN, and communications between the ONS 15327 and CTC might be affected. The network management LAN is the data network connecting the workstation running the CTC software to the XTC card. The problem causing the alarm is external to the ONS 15327.

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

Clear the EXCCOL Alarm

Step 1 Verify that the network device port connected to the XTC 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 XTC 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).

2.6.54 EXERCISE-RING-REQ

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

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

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

2.6.55 EXERCISE-SPAN-REQ

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

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

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

2.6.56 EXT

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

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

Note The REM LED is triggered when an EXT alarm is raised.

Clear the EXT Alarm

Step 1 In node view, click the **Maintenance** tab to gather further information about the EXT alarm.

Step 2 Perform your standard operating procedure for the environmental condition.

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).

2.6.57 EXTRA-TRAF-PREEMPT

- Major (MJ), Service Affecting (SA)

An Extra Traffic Preempted (EXTRA-TRAF-PREEMPT) alarm occurs on OC-N cards in two-fiber BLSRs because low-priority traffic directed to the protect system has been preempted by a working system protection switch.

Clear the EXTRA-TRAF-PREEMPT Alarm

Step 1 Verify that the protection switch has occurred by checking the Conditions tab.

Step 2 If a ring switch has occurred, clear the alarm on the working system by following the appropriate alarm procedure 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).

2.6.58 FAILTOSW

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

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

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the FAILTOSW Condition

Step 1 Look up and troubleshoot the higher-priority alarm. Clearing the higher-priority condition frees the 1:N electrical card or 1+1 optical card and clears the FAILTOSW.

Step 2 If the condition does not clear, replace the working card that is reporting the higher priority alarm by following the "Physically Replace a Card" procedure on page 2-130. This card is the working optical card using the 1+1 protection and not reporting FAILTOSW.

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

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

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).

2.6.59 FAILTOSW-PATH

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

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

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the FAILTOSW-PATH Condition in a Path Protection Configuration

Step 1 Look up and clear the higher priority alarm. Clearing this alarm frees the standby card and clears the FAILTOSW-PATH condition.

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

Step 2 If the condition does not clear, replace the active OC-N card that is reporting the higher priority alarm. Complete the "Physically Replace a Card" procedure on page 2-130. 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 alarm.

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

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).

2.6.60 FAILTOSWR

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

The Fail to Switch to Protection Ring (FAILTOSWR) 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 condition (see page 2-104) or an SF condition (see page 2-106)] clears.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the FAILTOSWR Condition in a 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 drop-down menu.

Step 2 If the condition does not clear, in 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 in service (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 correct, 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 in service (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 externally 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 15327 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 1-77 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 2-130 for the protect standby OC-N card.

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

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

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

2.6.61 FAILTOSWS

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

The Failure to Switch to Protection Span (FAILTOSWS) condition signals an APS span switch failure. 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 an SD condition (see page 2-104) or SF condition (see page 2-106) causing an APS switch clears.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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 drop-down menu.

Step 2 If the condition does not clear, in 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 (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 in service (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 correct, 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 in service (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 15327 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 1-77 lists these specifications.

Step 11 Repeat Steps 6 through 10 for any other ports on the card.

Step 12 If the optical power level for all OC-N cards is within specifications, complete the "Physically Replace a Card" procedure on page 2-130 for the protect standby OC-N card.

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

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

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

2.6.62 FAN

- Critical (CR), Service Affecting (SA)

The Fan Failure (FAN) alarm indicates a problem with the fan-tray assembly. When the fan-tray assembly is not fully functional, the temperature of the ONS 15327 can rise above its normal operating range.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the FAN Alarm

Step 1 Verify whether the air filter needs replacement. Complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 3-3.

Step 2 If the filter is clean, complete the "Remove and Reinsert Fan-Tray Assembly" procedure on page 2-131.

Note The fan-tray assembly 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 3-1.

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).

2.6.63 FANDEGRADE

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

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

Clear the FANDEGRADE Alarm

Step 1 Complete the "Clear the FAN Alarm" procedure on page 2-60.

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).

2.6.64 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) alarm (see page 2-84) downstream.

Clear the FE-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-16.

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).

2.6.65 FE-DS1-MULTLOS

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

The Far-End Multiple DS-1 LOS Detected (FE-DS1-MULTLOS) condition occurs when multiple DS-1 signals are lost at the far-end node.

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 condition or condition by troubleshooting the main alarm at its source. Both alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-MULTLOS Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition.

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).

2.6.66 FE-DS1-NSA

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

The Far End DS-1 Equipment Failure Non-Service Affecting (FE-DS1-NSA) condition occurs when a far-end XTC 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.

Clear the FE-DS1-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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).

2.6.67 FE-DS1-SA

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

The Far End DS-1 Equipment Failure Service Affecting (FE-DS1-SA) condition occurs when there is a far-end equipment failure on an XTC 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.

Clear the FE-DS1-SA Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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).

2.6.68 FE-DS1-SNGLLOS

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

The Far-End Single DS-1 LOS(FE-DS1-SNGLLOS) condition occurs when a single DS-1 signal is lost on a far-end XTC card. Signal loss also causes an LOS (OC-N) alarm (see page 2-84).

The prefix FE 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.

Clear the FE-DS1-SNGLLOS Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE condition.

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).

2.6.69 FE-DS3-NSA

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

The Far End DS-3 Equipment Failure Non-Service Affecting (FE-DS3-NSA) condition occurs when a far-end XTC-28-3 card 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.

Clear the FE-DS3-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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).

2.6.70 FE-DS3-SA

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

The Far End DS-3 Equipment Failure Service Affecting (FE-DS3-SA) condition occurs when there is a far-end equipment failure on an XTC-28-3 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 condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both alarms or conditions clear when the main alarm clears.

Clear the FE-DS3-SA Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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).

2.6.71 FE-EQPT-NSA

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

The Far End Common Equipment Failure Non-Service Affecting (FE-EQPT-NSA) condition occurs when a non-service affecting equipment failure is detected on a far-end XTC card.

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 condition 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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the FE-EQPT-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE condition.

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-EXERCISING-RING

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

The Far End Exercising Ring (FE-EXERCISING-RING) condition occurs when far-end optical (traffic) cards in a two-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.

2.6.73 FE-EXERCISING-SPAN

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

The Far End Exercising Span (FE-EXERCISING-SPAN) condition occurs when far-end optical (traffic) cards in a 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.

2.6.74 FE-FRCDWKSWPR-RING

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

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

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

Clear the FE-FRCDWKSWPR-RING Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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 2-127 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).

2.6.75 FE-FRCDWKSWPR-SPAN

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

The Far End Working Facility Forced to Switch to Protection Span (FE-FRCDWKSWPR-SPAN) condition occurs from a far-end node when a span on a 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.

Clear the FE-FRCDWKSWPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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 2-127 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).

2.6.76 FE-IDLE

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

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

The prefix FE 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 condition or condition by troubleshooting the main alarm at its source. Both alarms clear when the main alarm clears.

Clear the FE-IDLE Condition

Step 1 To troubleshoot the FE condition, determine which node and card links directly to the card reporting the FE condition.

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 2-127.

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-LOCKOUTOFPR-SPAN

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

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

Clear the FE-LOCKOUTOFPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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 2-127 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).

2.6.78 FE-LOF

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

The Far End LOF (FE-LOF) condition occurs when a far-end node reports an LOF (DS-3) alarm (see page 2-79).

The prefix FE 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 condition or condition by troubleshooting the main alarm at its source. Both alarms or conditions clear when the main alarm clears.

Clear the FE-LOF Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE condition.

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

Step 3 Complete the "Clear the LOF (DS-3) Alarm" procedure on page 2-79. The procedure 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).

2.6.79 FE-LOS

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

The Far End LOS (FE-LOS) condition occurs when a far-end node reports an LOS (DS-3) alarm (see page 2-83).

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.

Clear the FE-LOS Condition

Step 1 To troubleshoot the FE condition, determine which node and card links directly to the card reporting the FE condition.

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 2-78.

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).

2.6.80 FE-MANWKSWPR-RING

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

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

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

Clear the FE-MANWKSWPR-RING Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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 2-127.

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-MANWKSWPR-SPAN

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

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

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

Clear the FE-MANWKSWPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card links directly to the card reporting the FE alarm.

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 2-127.

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 FEPRLF

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

The Far End Protection Line Failure (FEPRLF) alarm occurs when an APS channel SF condition (see page 2-106) occurs on the protect card coming into the node.

Note The FEPRLF alarm occurs only on the ONS 15327 when bidirectional protection is used on optical (traffic) cards in a 1+1 configuration or BLSR configuration.

Clear the FEPRLF Alarm on a BLSR

Step 1 To troubleshoot the FE condition, determine which node and card links directly to the card reporting the FE alarm.

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).

2.6.83 FORCED-REQ

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

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

Clear the FORCED-REQ Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" 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).

2.6.84 FORCED-REQ-RING

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

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

Clear the FORCED-REQ-RING Condition

Step 1 Complete the "Clear the FORCED-REQ Condition" procedure on page 2-69.

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).

2.6.85 FORCED-REQ-SPAN

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

The Force Switch Request Span (FORCED-REQ-SPAN) condition applies to optical trunk cards in BLSRs when the FORCE SPAN command is applied to a BLSR to force traffic from working to protect or from protect to working.

Clear the FORCED-REQ-SPAN Condition

Step 1 Complete the "Clear the FORCED-REQ Condition" procedure on page 2-69.

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).

2.6.86 FRCDSWTOINT

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

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

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

2.6.87 FRCDSWTOPRI

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

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

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

2.6.88 FRCDSWTOSEC

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

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

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

2.6.89 FRCDSWTOTHIRD

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

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

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

2.6.90 FRNGSYNC

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

The Free-Running Synchronization Mode (FRNGSYNC) alarm occurs when the reporting ONS 15327 is in free run synchronization mode. External timing sources have been disabled and the node is using its internal clock, or the ONS 15327 has lost its designated BITS timing source. After the 24-hour holdover period expires, timing slips might begin to occur on an ONS 15327 relying on an internal clock.

Clear the FRNGSYNC Alarm

Step 1 If the ONS 15327 is configured to operate from its internal clock, disregard the FRNGSYNC alarm.

Step 2 If the ONS 15327 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 a SYNCPRI alarm (see page 2-117) and a SYNCSEC alarm (see page 2-117).

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).

2.6.91 FSTSYNC

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

A Fast Start Synchronization mode (FSTSYNC) alarm occurs when the ONS 15327 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. The alarm does not require troubleshooting.

2.6.92 FULLPASSTHR-BI

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

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

Clear the FULLPASSTHR-BI Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" 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).

2.6.93 HITEMP

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

The High Temperature (HITEMP) alarm occurs when the temperature of the ONS 15327 is above 122° F (50° C).

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the HITEMP Alarm

Step 1 Verify that the environmental temperature of the room is not abnormally high.

Step 2 If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15327.

Step 3 If airflow is not blocked, physically ensure that blank faceplates fill the ONS 15327 empty slots. Blank faceplates help airflow.

Step 4 If faceplates fill the empty slots, verify whether the air filter needs replacement. Refer to "Inspect and Maintain the Air Filter" procedure in the *Cisco ONS 15327 Procedure Guide*.

Step 5 If the filter is clean, complete the "Remove and Reinsert Fan-Tray Assembly" procedure on page 2-131.

Note The fan-tray assembly should run immediately when correctly inserted.

Step 6 If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 3-1.

Step 7 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 the alarm applies to the NE, or a non-service-affecting problem if the alarm applies to equipment.

2.6.94 HLDOVRSYNC

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

The Holdover Synchronization Mode (HLDOVRSYNC) alarm indicates a loss of the primary or secondary timing reference. Timing reference loss occurs when line coding (AMI, B8ZS) on the timing input is different from the configuration on the ONS 15327. It also usually occurs during the selection of a new node reference clock. The HLDOVRSYNC alarm indicates that the ONS 15327 has gone into holdover and is using the ONS 15327 internal reference clock, which is a Stratum 3-level timing device. The alarm clears when primary or secondary timing is reestablished.

Clear the HLDOVRSYNC Alarm

Step 1 Clear additional alarms that relate to timing, such as a FRNGSYNC condition (see page 2-71); a FSTSYNC condition (see page 2-71); a HLDOVRSYNC alarm (see page 2-73); an LOF (BITS) alarm (see page 2-77); an LOS (BITS) alarm (see page 2-81); a MANSWTOINT condition (see page 2-88); a MANSWTOPRI condition (see page 2-89); a MANSWTOSEC condition (see page 2-89); a MANSWTOTHIRD condition (see page 2-89); a SWTOPRI condition (see page 2-115); a SWTOSEC condition (see page 2-115); a SWTOTHIRD condition (see page 2-116); a SYNC-FREQ condition (see page 2-116); a SYNCPRI alarm (see page 2-117); a SYNCSEC alarm (see page 2-117); or a SYNCTHIRD alarm (see page 2-118).

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).

2.6.95 IMPROPRMVL

- Critical (CR), Service Affecting (SA)

The Improper Removal (IMPROPRMVL) alarm occurs when a card is physically removed from its slot before it is deleted from CTC. The card does not need to be in service to cause the IMPROPRMVL alarm; it only needs to be recognized by CTC. The alarm does not appear if you delete the card from CTC before you physically remove the card from the node.

Caution Updating software on a standby XCT card can take up to 30 minutes.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Note CTC gives the user approximately 15 seconds to physically remove the card before CTC begins a card reboot.

Clear the IMPROPRMVL Alarm

Step 1 In node view, right-click the card reporting the IMPROPRMVL.

Step 2 Choose **Delete** from the shortcut menu.

Note CTC does not allow you to delete the reporting card if the card is in service, has a circuit mapped to it, is paired in a working protection scheme, has DCC enabled, or is used as a timing reference.

Step 3 If any ports on the card are in service, take them out of service:

Caution Before taking a port out of service, ensure that no live traffic is present.

a. In CTC, 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 4 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-128.

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 > SONET DCC** tabs.
b. Click the slots and ports listed in DCC terminations.
c. Click **Delete** and click **Yes** in the dialog box that appears.

Step 7 If the card is used as a timing reference, change the timing reference:

a. Click the **Provisioning > Timing** tabs.
b. Under NE Reference, click the drop-down 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).

2.6.96 INC-ISD

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

The DS-3 Idle (INC-ISD) condition indicates that the XTC-28-3 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.

2.6.97 INHSWPR

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

The Inhibit Switch To Protect Request on Equipment (INHSWPR) condition occurs on traffic cards when the ability to switch to protect has been disabled. If the card is part of a 1+1 protection scheme, traffic remains locked onto the working system.

Clear the INHSWPR Condition

Step 1 Complete the "Clear an External Switching Command" procedure on page 2-128.

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).

2.6.98 INHSWWKG

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

The Inhibit Switch To Working Request on Equipment (INHSWWKG) condition occurs on traffic cards when the ability to switch to working has been disabled. If the card is part of a 1+1 protection scheme, traffic remains locked onto the protect system.

Clear the INHSWWKG Condition

Step 1 Complete the "Clear an External Switching Command" procedure on page 2-128.

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 INVMACADR

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

The Equipment Failure Invalid MAC Address (INVMACADR) alarm occurs when the ONS 15327 MAC Address is invalid. The MAC Address is permanently assigned to the ONS 15327 chassis when it is manufactured. Do not attempt to troubleshoot an INVMACADR. Contact TAC at 1-800-553-2447.

2.6.100 KB-PASSTHR

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

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

Clear the KB-PASSTHR Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" 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).

2.6.101 LKOUTPR-S

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

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

Clear the LKOUTPR-S Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" 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).

2.6.102 LOCKOUT-REQ

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

The Lock Out Switch Request on Facility/Equipment (LOCKOUT-REQ) 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 at the path level. A lock out prevents protection switching. Clearing the lock out again allows protection switching and clears the LOCKOUT-REQ condition.

Clear the LOCKOUT-REQ Condition

Step 1 Complete the "Clear a Path Protection Lock Out" procedure on page 2-128.

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).

2.6.103 LOCKOUT-REQ-RING

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

The Lock Out Switch Request Ring (LOCKOUT-REQ-RING) condition occurs when a LOCKOUT RING command is applied to a BLSR to prevent all protection switching on the ring.

Clear the LOCKOUT-REQ-RING Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" 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).

2.6.104 LOF (BITS)

- Major (MJ), Service Affecting (SA)

The Loss of Frame (LOF) BITS alarm occurs when a port on the XTC BITS input detects an LOF on the incoming BITS timing reference signal. LOF indicates that the receiving ONS 15327 has lost frame delineation in the incoming data.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Note The procedure assumes that the BITS timing reference signal is functioning properly. It also assumes that the alarm is not appearing during node turn up.

Clear the LOF (BITS) Alarm

Step 1 Verify that the framing and line coding match between the BITS input and the XTC:

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

b. Find the framing and coding 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 the Coding field matches the coding of the BITS timing source (B8ZS or AMI).

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

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

g. If the framing does not match, click **Framing** and choose the appropriate framing from the drop-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 XTC, complete the "Physically Replace a Card" procedure on page 2-130 for the XTC card.

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

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).

2.6.105 LOF (DS-1)

- Major (MJ), Service Affecting (SA)

The DS-1 LOF alarm indicates that the receiving ONS 15327 has lost frame delineation in an incoming DS-1 data stream.

Clear the LOF (DS-1) Alarm

Step 1 Verify that the line framing and line coding match between the DS-1 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 XTC.

d. Click the **Provisioning > DS1 > 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 drop-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 drop-down menu.

g. If the signal source line coding does not match the reporting port, click the **Line Coding** column and choose the appropriate type from the drop-down menu.

h. Click **Apply**.

Note On the DS-1 Line tab, the B8ZS coding field is normally paired with ESF in the Line Type field. AMI coding is normally paired with D4 in the Line Type field.

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).

2.6.106 LOF (DS-3)

- Critical (CR), Service Affecting (SA)

The DS-3 LOF alarm indicates that the receiving ONS 15327 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 15327. On XTC-28-3 cards, the alarm occurs only on DS-1 lines with the provisionable framing format set to SF (D4) and not on cards with the provisionable framing format set to unframed.

Clear the LOF (DS-3) Alarm

Step 1 Change the line type of the non-ONS equipment attached to the reporting card to D4:

a. Display the card view of the reporting card.

b. Click the **Provisioning > DS1 > 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 **D4** from the drop-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).

2.6.107 LOF (OC-N)

- Critical (CR), Service Affecting (SA)

The OC-N LOF alarm occurs when a port on the reporting OC-N card has an LOF condition. LOF indicates that the receiving ONS 15327 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.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the LOF (OC-N) Alarm

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

Step 2 If cabling continuity is correct, clean the fiber connectors according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15327 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).

2.6.108 LOP-P

- Critical (CR), Service Affecting (SA)

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

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

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the LOP-P Alarm

Step 1 In node view, click the **Circuits** tab and view the alarmed circuit.

Step 2 Verify that the correct circuit size is 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 2-128.

Step 5 Recreate the circuit for the correct size. For instructions, see the *Cisco ONS 15327 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).

2.6.109 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.

Clear the LOP-V Alarm

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-81.

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).

2.6.110 LOS (BITS)

- Major (MJ), Service Affecting

The BITS LOS alarm indicates that the XTC card has an LOS from the BITS timing source. The LOS (BITS-N) means that 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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the LOS (BITS) Alarm

Step 1 Verify the wiring connection from the BITS clock pin fields on the ONS 15327 MIC to the timing source.

Step 2 If wiring is correct, 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).

2.6.111 LOS (DS-1)

- Major (MJ), Service Affecting (SA)

A DS-1 LOS alarm for a DS-3 port or a DS-1 port occurs when the XTC port 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.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the LOS (DS-1) Alarm

Step 1 Verify cabling continuity to the port.

Step 2 If the cabling is correct, verify that the correct port is 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 in service (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 MIC card.

Step 6 Repeat Steps 1 through 5 for any other port on the card that reports the LOS.

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, or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting card.

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).

2.6.112 LOS (DS-3)

- Critical (CR), Service Affecting (SA)

The DS-3 LOS alarm for either an XTC DS-3 port or 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.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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.

Clear the LOS (DS-3) Alarm

Step 1 Verify cabling continuity to the port.

Step 2 If the cabling is correct, verify that the correct port is in service (IS):

Step 3 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.

f. To determine whether the OC-N port is in service, double-click the card in CTC to display the card view.

g. Click the **Provisioning > Line** tabs.

h. Verify that the **State** column lists the port as IS.

i. If the State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Step 4 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 5 If the signal is valid, ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected.

Step 6 If a valid signal exists, replace the DS-N connector on the MIC card.

Step 7 Repeat Steps 1 through 5 for any other port on the card that reports the LOS.

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, or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting card.

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

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).

2.6.113 LOS (OC-N)

- Critical (CR), Service Affecting (SA)

An OC-N LOS alarm 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 **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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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.

Clear the LOS (OC-N) Alarm

Step 1 Verify fiber continuity to the port.

Step 2 If the cabling is correct, 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 in service (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 connectors according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15327 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 1-77 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 Repeat Steps 1 through 5 for any other port on the card reporting the alarm.

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, or if clearing an alarm did not clear the LOS (OC-N), complete the "Physically Replace a Card" procedure on page 2-130 for the reporting card.

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).

2.6.114 LPBKCRS

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

The Loopback XTC (LPBKCRS) condition indicates that there is a software cross-connect loopback active between a traffic card and an XTC 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 1-4.

Clear the LBKCRS Condition

Step 1 To remove the loopback cross-connect condition, double-click the traffic 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.

2.6.115 LPBKFACILITY (DS-N)

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

A DS-N Loopback Facility (LPBKFACILITY) 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 a DS-N Circuit Path" section on page 1-4.

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

Note XTC-28-3 cards only support facility loopbacks on DS-1 circuits.

Clear the LPBKFACILITY (DS-N) Condition

Step 1 From the node view, double-click the reporting XTC-28-3 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 2-129.

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).

2.6.116 LPBKFACILITY (OC-N)

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

An OC-N 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 1-21.

Clear the LPBKFACILITY (OC-N) Condition

Step 1 Complete the "Clear a Loopback" procedure on page 2-129.

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 nonlooped path to log into the node after the loopback is applied, thus enabling you to remove the facility loopback. Ensuring a second DCC is not necessary if you are directly connected to the ONS 15327 containing the loopback OC-N.

2.6.117 LPBKTERMINAL (DS-N, OC-N)

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

A DS-N or OC-N Loopback Terminal (LPBKTERMINAL) 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.

Note Terminal loopback is not supported at the DS1 level for the XTC-28-3 card.

Clear the LPBKTERMINAL (DS-N, OC-N) Condition

Step 1 Complete the "Clear a Loopback" procedure on page 2-129.

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).

2.6.118 LPBKTERMINAL (G-Series)

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

A G-Series 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 G1000-2 card, the outgoing signal is not transmitted; it is only redirected in the receive direction. G1000-2 cards only support terminal loopbacks.

For more information about loopbacks, see the "Network Troubleshooting Tests" section on page 1-2.

Clear the LPBKTERMINAL (G-Series) Condition

Step 1 Complete the "Clear a Loopback" procedure on page 2-129.

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 MAN-REQ

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

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

Clear the MAN-REQ Condition

Step 1 Complete the "Clear a Path Protection Lock Out" procedure on page 2-128.

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 MANRESET

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

A User-Initiated Manual Reset (MANRESET) 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.

2.6.121 MANSWTOINT

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

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

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

2.6.122 MANSWTOPRI

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

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

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

2.6.123 MANSWTOSEC

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

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

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

2.6.124 MANSWTOTHIRD

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

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

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

2.6.125 MANUAL-REQ-RING

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

The Manual Switch Request on Ring (MANUAL-REQ-RING) condition occurs when a user initiates a MANUAL RING command on two-fiber BLSR rings to switch from working to protect or protect to working.

Clear the MANUAL-REQ-RING Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" 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).

2.6.126 MANUAL-REQ-SPAN

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

The Manual Switch Request on Span (MANUAL-REQ-SPAN) condition occurs on BLSRs when a user initiates a MANUAL SPAN command to move BLSR traffic from a working span to a protect span.

Clear the MANUAL-REQ-SPAN Condition

Step 1 Complete the "Clear a BLSR Span Lock Out" 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).

2.6.127 MEA (EQPT)

- Critical (CR), Service Affecting (SA)

The Missing Equipment Attributes (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. Removing the incompatible cards clears the alarm.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the MEA (EQPT) Alarm

Step 1 Physically verify the type of card that sits in the slot reported in the Alarms window MEA alarm Object column.

Step 2 In CTC, click the **Inventory** tab to reveal the provisioned card type.

Step 3 If you prefer the card type depicted by CTC, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting card.

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

Step 4 If you prefer the card that physically occupies the slot and the card is not in service, has no circuits mapped, 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, 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 5 If any ports on the card are in service, take them out of service:

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 6 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-128.:

Caution Before deleting the circuit, ensure that live traffic is not present.

Step 7 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 8 Right-click the card reporting the alarm.

Step 9 Choose **Delete**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

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).

2.6.128 MEM-GONE

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

The Memory Gone (MEM-GONE) alarm occurs when data generated by software operations exceeds the memory capacity of the XTC card. CTC and the XTC card do 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).

2.6.129 MEM-LOW

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

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

2.6.130 MFGMEM

- Critical (CR), Service Affecting (SA)

The Manufacturing Data Memory Failure (MFGMEM) alarm occurs if the ONS 15327 cannot access the data in the electronically erasable programmable read-only memory (EEPROM). Either the memory module on the component failed or the XTC lost the ability to read that module. The EEPROM stores manufacturing data that is needed for both compatibility and inventory issues. An inability to read a valid MAC address disrupts IP connectivity and grays out the ONS 15327 icon on the CTC network view.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the MFGMEM (BP, Fan-Tray Assembly) Alarm

Step 1 Complete the "Reset the Active XTC Card in CTC" procedure on page 2-129.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

Step 3 If the MFGMEM alarm continues to report after replacing the XTC 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 3-1.

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).

2.6.131 NOT-AUTHENTICATED

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

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when it fails to log into a node. This alarm only displays in CTC where the login failure occurred.

Note NOT-AUTHENTICATED is an informational alarm and is resolved when CTC successfully logs into the node.

2.6.132 PDI-P

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

A PDI Path (PDI-P) 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 15327 encounters an SLMF when the payload, such as an ATM, does not match what the signal label is reporting. An AIS condition (see page 2-16) often accompanies the PDI-P condition. If the PDI-P is the only condition reported with the AIS condition (see page 2-16), 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 G1000-2 card circuit might result from the end-to-end Ethernet link integrity feature of the G1000-2. If the link integrity is the cause, it typically is accompanied by an a TPTFAIL (G-Series) alarm (see page 2-120) or a CARLOSS (G Series) alarm (see page 2-34) 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.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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 up to ten minutes for the ONS 15327 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 2-128.

Caution Deleting a circuit might affect traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15327 Procedure Guide* for detailed procedures to create circuits.

Step 5 If circuit deletion and recreation does not clear the condition, verify that the far-end OC-N card providing STS payload to the reporting card is not errored.

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 15327 Procedure Guide*.

Step 8 If the condition does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the optical/electrical cards.

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

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).

2.6.133 PEER-NORESPONSE

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

The Peer Card Not Responding (PEER-NORESPONSE) alarm is raised by the switch agent if either traffic card in a protection group does not receive a response to the peer status request message. PEER-NORESPONSE is a software failure and occurs at the task level, as opposed to a communication failure, which is a hardware failure between peer cards.

Clear the PEER-NORESPONSE Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-130 for the protect 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" (loading) 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 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, 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 2-130 for the working 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 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, 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).

2.6.134 PLM-P

- Critical (CR), Service Affecting (SA)

A Payload Label Mismatch Path (PLM-P) alarm indicates that signal does not match its label. The condition occurs due to an invalid C2 byte value in the SONET path overhead.

For example, this alarm can occur when a card is expecting a 0 value in the C2 byte, but receives a 4 instead. This can occur on the XTC card when the card expects a DS-1 signal but receives a DS-3 signal. The DS-3 signal C2 byte value is 4, so this will cause a label mismatch and a PLM-P alarm.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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 up to ten minutes for the ONS 15327 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 2-128.

Caution Deleting a circuit might affect traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15327 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 XTC card.

Step 6 If the alarm does not clear, verify the cross-connect between the OC-N card and the XTC 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 15327 Procedure Guide*.

Step 8 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the reporting traffic card.

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).

2.6.135 PLM-V

- Minor (MN), Service Affecting (SA)

A Payload Label Mismatch VT Layer (PLM-V) alarm indicates that the content of the V5 byte in the SONET overhead is inconsistent or invalid. PLM-V occurs when ONS nodes interoperate with equipment that performs bit-synchronous mapping for DS-1. ONS nodes use asynchronous mapping.

Clear the PLM-V Alarm

Step 1 Verify that your signal source matches the signal allowed by the traffic card. For example, the traffic card does not allow VT6 or VT9 mapping.

Step 2 If the signal source matches the card, verify that the SONET VT path originator is sending the correct VT label value. You can find the SONET VT path originator using circuit provisioning steps.

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

2.6.136 PRC-DUPID

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

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

The Procedural Error Duplicate Node ID (PRC-DUPID) alarm indicates that two identical node IDs exist in the same ring. The ONS 15327 requires each node in the ring to have a unique node ID.

Clear the PRC-DUPID Alarm

Step 1 Log into a node on the ring.

Step 2 Find the node ID by completing the "Identify a Ring ID or Node ID Number" procedure on page 2-126.

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 2-126 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).

2.6.137 PROTNA

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

The Protection Unit Not Available (PROTNA) alarm is caused by an OOS or failed protection card when an XTC 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.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the PROTNA Alarm

Step 1 If the PROTNA alarm occurs and does not clear, and if the alarm is raised against an XTC, ensure that there is a redundant control card installed and provisioned in the chassis.

Step 2 If the alarm is raised against a traffic card, verify whether the ports have been taken out of service:

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 ports.

d. Choose **OOS** to take the ports out of service.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-130 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 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, 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) a Card" procedure on page 2-130 for the reporting card.

Step 6 If you reinsert a high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

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).

2.6.138 PWR-A

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

An NE Power Failure at Connector A alarm indicates that the power is out of the specified 48 VDC input range and is either too high (overvoltage) or too low (undervoltage), requiring you to check the incoming power feed or separate power distribution equipment, or both. The PWR-A alarm may also be raised before actual loss of power in a discharging power plant problem and before full loss of incoming power.

Overvoltage or undervoltage can be caused by incoming DC power problems such as power rectifier failure, faulty power cabling, or a blown fuse.

Cisco encourages the use of separate DC power feeds from separate DC power plants or AC power rectifiers to ensure power redundancy to the feeds. Using a single DC power source for both MIC-A/PWR-A and MIC-B/PWR-B creates a risk through the single point of possible failure. Using dual power feeds removes this risk liability.

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.**

Clear the PWR-A Alarm

Step 1 Determine whether the PWR-A alarm is occurring alone or in conjunction with the PWR-B alarm, and determine whether MIC A and MIC B are using one single or two separate power supplies.

Step 2 If you are using separate power sources for the MIC A and MIC B power connectors and the PWR-A alarm occurs without the PWR-B alarm, inspect the incoming voltage to the MIC A connector using site practices. The alarm can be caused by problems such as power rectifier failure, faulty power cabling, or a blown fuse, and correct these issues. Solve these problems before continuing.

You can verify the power connection continuity and the power source output with a voltmeter using the procedures in the *Cisco ONS 15327 Procedure Guide*.

Step 3 If you are using a single power source for both the MIC A and MIC B cards and only the PWR-A alarm is occurring, an electrical cable continuity or connection problem may be to blame. Check for these problems and correct them if necessary.

Step 4 If you are using separate power sources for each MIC card and the PWR-A alarm occurs in conjunction with the PWR-B alarm, it is likely that both incoming power feeds or power plants are failing. Check for these problems according to site practice and correct as necessary.

Step 5 If you are using a single power source for both MIC cards and both the PWR-A and PWR-B alarms are raised, problems with both power feeds may be to blame, but a power plant failure is more likely. Check for these problems according to site practice and correct as necessary.

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).

2.6.139 PWR-B

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

An NE Power Failure at Connector B alarm indicates that the power is out of the specified 48 VDC input range and is either too high (overvoltage) or too low (undervoltage), requiring you to check the incoming power feed or separate power distribution equipment, or both. The PWR-B alarm may also be raised before actual loss of power in a discharging power plant problem and before full loss of incoming power.

Overvoltage or undervoltage can be caused by incoming DC power problems such as power rectifier failure, faulty power cabling, or a blown fuse.

Cisco encourages the use of separate DC power feeds from separate DC power plants or AC power rectifiers to ensure power redundancy to the feeds. Using a single DC power source for both MIC-A/PWR-A and MIC-B/PWR-B creates a risk through the single point of possible failure. Using dual power feeds removes this risk liability.

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.**

Clear the PWR-B Alarm

Step 1 Determine whether the PWR-B alarm is occurring alone or in conjunction with the PWR-A alarm, and determine whether MIC A and MIC B are using one single or two separate power supplies.

Step 2 If you are using separate power sources for the MIC A and MIC B power connectors and the PWR-B alarm occurs without the PWR-A alarm, inspect the incoming voltage to the MIC B connector using site practices. The alarm can be caused by problems such as power rectifier failure, faulty power cabling, or a blown fuse, and correct these issues. Solve these problems before continuing.

You can verify the power connection continuity and the power source output with a voltmeter using the procedures in the *Cisco ONS 15327 Procedure Guide*.

Step 3 If you are using a single power source for both the MIC A and MIC B cards and only the PWR-B alarm is occurring, an electrical cable continuity or connection problem may be to blame. Check for these problems and correct them if necessary.

Step 4 If you are using separate power sources for each MIC card and the PWR-B alarm occurs in conjunction with the PWR-A alarm, it is likely that both incoming power feeds or power plants are failing. Check for these problems according to site practice and correct as necessary.

Step 5 If you are using a single power source for both MIC cards and both the PWR-A and PWR-B alarms are raised, problems with both power feeds may be to blame, but a power plant failure is more likely. Check for these problems according to site practice and correct as necessary.

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).

2.6.140 PWR-REDUN

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

The Redundant Power Capability Lost (PWR-REDUN) alarm applies to cards that have two built-in fuses (such as newer optical 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.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the PWR-REDUN Alarm

Step 1 The card fuse is not field-replaceable. Complete the "Physically Replace a Card" procedure on page 2-130.

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

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.

2.6.141 RAI

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

The Remote Alarm Indication (RAI) condition signifies an end-to-end failure. The error condition is sent from one end of the SONET path to the other. RAI on the DS3XM-6 card indicates that the far-end node is receiving a DS-3 AIS condition (see page 2-16).

Clear the RAI Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-16.

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).

2.6.142 RCVR-MISS

- Major (MJ), Service Affecting (SA)

A Facility Termination Equipment Receiver Missing (RCVR-MISS) alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its connector. Incorrect impedance usually occurs when a receive cable is missing from the XTC DS-1 port or a possible mismatch of equipment occurs.

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.**

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the RCVR-MISS Alarm

Step 1 Ensure that the device attached to the XTC port is operational.

Step 2 If the attachment is correct, verify that the cabling is securely connected.

Step 3 If the cabling is correct, 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).

2.6.143 RFI-L

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

A Remote Fault Indication (RFI) Line condition occurs when the ONS 15327 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-L condition in the reporting node. RFI-L indicates that the condition is occurring at the line level.

Clear the RFI-L Condition

Step 1 Log into the node at the far-end node of the reporting ONS 15327.

Step 2 Verify whether there are other alarms, especially an LOS (OC-N) alarm (see page 2-84).

Step 3 Clear the alarms; to clear an LOS (OC-N) alarm (see page 2-84), refer to the LOS section in this chapter.

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 RFI-P

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

An RFI Path condition occurs when the ONS 15327 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P condition in the reporting node. RFI-P occurs in the node that terminates a path.

Clear the RFI-P Condition

Step 1 Verify that the ports are enabled and in service (IS) on the reporting ONS 15327:

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 in service (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 alarm (see page 2-122) or an UNEQ-V alarm (see page 2-124).

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).

2.6.145 RFI-V

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

An RFI VT Layer condition occurs when the ONS 15327detects 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.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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 15327 Procedure Guide*.

Step 2 If connectors are correctly connected, verify that the XTC 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 whether the signal source has 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 15327.

Step 5 Clear alarms in the far-end node, especially an UNEQ-P alarm (see page 2-122) or an UNEQ-V alarm (see page 2-124).

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).

2.6.146 RING-MISMATCH

- Major (MJ), Service Affecting (SA)

A Procedural Error Mismatch Ring (RING-MISMATCH) alarm occurs when the ring ID of the ONS 15327 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.

Clear the RING-MISMATCH Alarm

Step 1 In 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 2-126.

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 2-126.

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).

2.6.147 RING-SW-EAST

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

The Ring Switch is Active East Side (RING-SW-EAST) condition occurs when a ring switch occurs at the east side of two-fiber BLSR. The condition clears when the switch is cleared.

Note RING-SW-EAST is an informational condition. It does not require troubleshooting.

2.6.148 RING-SW-WEST

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

The Ring Switch is Active West Side (RING-SW-WEST) condition occurs when a ring switch occurs at the west side of a two-fiber BLSR. The condition clears when the switch is cleared.

Note RING-SW-WEST is an informational condition. It does not require troubleshooting.

2.6.149 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 15327 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 **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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the SD Condition

Step 1 Complete the "Verify BER Threshold Level" procedure on page 2-130.

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 the level is within guidelines.

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

Step 3 If the optical power level is correct, verify that optical receive levels are within the acceptable range.

Step 4 If receive levels are correct, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the *Cisco ONS 15327 Procedure Guide*.

Step 5 If the alarm 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).

2.6.150 SD-L

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

An SD Line condition is similar to an SD condition (see page 2-104). It applies to the line level of the SONET signal.

Clear the SD-L Condition

Step 1 Complete the "Clear the SD Condition" 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 (1-800-553-2447).

2.6.151 SD-P

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

An SD Path (SD-P) condition is similar to an SD condition (see page 2-104) 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 circuits, the BER threshold on the ONS 15327 is user provisionable and has a range for SD from 10^{-9} to 10^{-5}. For BLSR 1+1 and unprotected circuits, the BER threshold value is not user provisionable and the error rate is hard-coded to 10^{-6}.

On path protection, an SD-P condition causes a switch from the working card to the protect card at the path (STS) level. On BLSR 1+1 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.

Clear the SD-P Condition

Step 1 Complete the "Clear the SD Condition" 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 (1-800-553-2447).

2.6.152 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 condition (see page 2-104) 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 15327 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.

Clear the SF Condition

Step 1 Complete the "Clear the SD Condition" 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 (1-800-553-2447).

2.6.153 SF-L

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

An SF Line (SF-L) condition is similar to an SF condition (see page 2-106) but it applies to the line layer of the signal.

Clear the SF-L Condition

Step 1 Complete the "Clear the SD Condition" 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 (1-800-553-2447).

2.6.154 SF-P

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

An SF Path (SF-P) condition is similar to an SF condition (see page 2-106), 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 circuits, the BER threshold on the ONS 15327 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, 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.

Clear the SF-P Condition

Step 1 Complete the "Clear the SD Condition" 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 (1-800-553-2447).

2.6.155 SFTWDOWN

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

A Software Download in Progress (SFTWDOWN) alarm occurs when the XTC 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 XTC card.

Note SFTWDOWN is an informational alarm.

2.6.156 SNTP-HOST

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

The Simple Network Timing Protocol (SNTP) Host Failure (SNTP-HOST) 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.

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 15327.

Step 3 If no network problems exist, ensure that the ONS 15327 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 the box.

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 15327 Reference Manual* for more information about 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).

2.6.157 SPAN-SW-EAST

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

The Span Switch is Active East Side (SPAN-SW-EAST) condition occurs when a span switch occurs at the east side of a BLSR span. The condition clears when the switch is cleared.

Note SPAN-SW-EAST is an informational condition. It does not require troubleshooting.

2.6.158 SPAN-SW-WEST

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

The Span Switch is Active West Side (SPAN-SW-WEST) condition occurs when a span switch occurs at the west side of a BLSR span. The condition clears when the switch is cleared.

Note SPAN-SW-EAST is an informational condition. It does not require troubleshooting.

2.6.159 SQUELCH

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

The Ring Squelching Traffic (SQUELCH) condition occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance FORCE RING commands. The isolation or failure of the node disables circuits that originate or terminate on the failed node. Squelch alarms appear on one or both of the nodes on either side of the isolated/failed node. The AIS-P condition (see page 2-17) also appears on all nodes in the ring except the isolated node.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the SQUELCH Condition

Step 1 Determine the isolated node:

a. In 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 correct, verify that the proper ports are 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 in service (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 card's receiver specifications. Refer to the *Cisco ONS 15327 Reference Manual* for card specifications.

Step 6 If the receiver levels are correct, ensure that the optical transmit and receive fibers are connected properly.

Step 7 If the connectors are correct, complete the "Physically Replace a Card" procedure on page 2-130 for the OC-N card.

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

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).

2.6.160 SSM-DUS

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

The Synchronization Status Message (SSM) 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.

2.6.161 SSM-FAIL

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

The SSM Failed (SSM-FAIL) alarm occurs when the synchronization status messaging received by the ONS 15327 fails. The problem is external to ONS 15327. The ONS 15327 is set up to receive SSM, but the timing source is not delivering valid SSM messages.

Clear the SSM-FAIL Alarm

Step 1 Verify that SSM is enabled on the external timing source.

Step 2 If timing is enabled, use an optical test set to determine that the external timing source is delivering SSM.

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

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 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-quality.

Note SSM-LNC is an informational condition. It does not require troubleshooting.

2.6.163 SSM-OFF

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

The SSM Off (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 15327 is set up to receive SSM, but the timing source is not delivering SSM messages.

Clear the SSM-OFF Condition

Step 1 Complete the "Clear the SSM-FAIL Alarm" procedure on page 2-110.

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).

2.6.164 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-quality.

Note SSM-PRC is an informational condition. It does not require troubleshooting.

2.6.165 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.

2.6.166 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.

2.6.167 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.

2.6.168 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.

2.6.169 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.

2.6.170 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.

2.6.171 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.

2.6.172 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 15327 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 15327.

Clear the STU Condition

Step 1 In 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).

2.6.173 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.

2.6.174 SWMTXMOD

- Critical (CR), Service Affecting (SA)

The Switching Matrix Module Failure (SWMTXMOD) alarm occurs on the XTC card or a traffic card. If the alarm reports against a traffic card, it occurs when the logic component on the XTC 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 an XTC card, it occurs when a logic component internal to the reporting XTC card is out of frame with a second logic component on the same XTC card. One or more traffic cards might lose traffic as a result of the cross-connect frame failure.

Note The only way to switch the XTC protection group is to reset the active XTC.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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 2-130 for the card.

Step 2 If you reinsert a high-speed card, verify the following LED behavior:

- The FAIL LED blinks for approximately 30 seconds.
- All LEDs blink once and turn off.
- The ACT/STBY LED is green (active).

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 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, 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 2-130 for the standby cross-connect card.

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 alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-130 for the standby XTC card.

The reboot takes up to ten minutes.

Step 6 Complete the "Reset a Traffic Card in CTC" procedure on page 2-130 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 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 15327, the ACT/STBY LED is illuminated.
- If you are looking at the node view of the ONS 15327, 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) a Card" procedure on page 2-130 for the traffic card.

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).

2.6.175 SWTOPRI

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

The Synchronization Switch to Primary Reference (SWTOPRI) condition occurs when the ONS 15327 switches to the primary timing source (reference 1). The ONS 15327 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.

2.6.176 SWTOSEC

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

The Synchronization Switch to Secondary Reference (SWTOSEC) condition occurs when the ONS 15327 has switched to the secondary timing source (reference 2). The ONS 15327 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Clear the SWTOSEC Condition

Step 1 To clear the condition, clear alarms related to failures of the primary source, such as the SYNCPRI alarm (see page 2-117).

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 SWTOTHIRD

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

The Synchronization Switch to Third Reference (SWTOTHIRD) condition occurs when the ONS 15327 has switched to the third timing source (reference 3). The ONS 15327 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 a SYNCPRI alarm (see page 2-117) or a SYNCSEC alarm (see page 2-117).

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 SYNC-FREQ

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

The Synchronization Reference Frequency Out Of Bounds (SYNC-FREQ) condition is reported against any reference that is out of the bounds for valid references. The login node fails the reference and chooses another internal or external reference to use.

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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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 timing 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 2-130 for the XTC card.

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

Note The active XTC takes up to 30 minutes to transfer the system software to the newly installed XTC. Software transfer occurs in instances where different software versions exist on the two cards. During the transfer operation, the LEDs on the XTC flash fail and then the active/standby LED flashes. When the transfer completes, the XTC reboots and goes into standby mode after approximately three minutes.

Step 3 If the SYNC-FREQ alarm continues to report after replacing the XTC card, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

2.6.179 SYNCPRI

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

A Loss of Timing on Primary Reference (SYNCPRI) alarm occurs when the ONS 15327 loses the primary timing source (reference 1). The ONS 15327 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 15327 should switch to its secondary timing source (reference 2). Switching to the secondary timing source also triggers a SWTOSEC condition (see page 2-115).

Clear the SYNCPRI Alarm

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Verify the current configuration for the REF-1 of the NE Reference.

Step 3 If the primary reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-82.

Step 4 If the primary reference clock is an incoming port on the ONS 15327, complete the "Clear the LOS (OC-N) Alarm" procedure on page 2-85.

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).

2.6.180 SYNCSEC

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

A Loss of Timing on Secondary Reference (SYNCSEC) alarm occurs when the ONS 15327 loses the secondary timing source (reference 2). The ONS 15327 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 15327 should switch to the third timing source (reference 3) to obtain valid timing for the ONS 15327. Switching to the third timing source also triggers a SWTOTHIRD condition (see page 2-116).

Clear the SYNCSEC Alarm

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Verify the current configuration of the REF-2 for the NE Reference.

Step 3 If the secondary reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-82.

Step 4 Verify that the BITS clock is operating properly.

Step 5 If the secondary timing source is an incoming port on the ONS 15327, complete the "Clear the LOS (OC-N) Alarm" procedure on page 2-85.

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).

2.6.181 SYNCTHIRD

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

A Loss of Timing on Third Reference (SYNCTHIRD) alarm occurs when the ONS 15327 loses the third timing source (reference 3). The ONS 15327 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 15327 uses an internal reference for source three, the XTC card might have failed. The ONS 15327 often reports either a FRNGSYNC condition (see page 2-71) or a HLDOVRSYNC alarm (see page 2-73) after a SYNCTHIRD alarm.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the SYNCTHIRD Alarm

Step 1 In node view, click the **Provisioning > Timing** tabs.

Step 2 Verify the current configuration of the REF-3 for the NE Reference. For more information about references, refer to the *Cisco ONS 15327 Procedure Guide*.

Step 3 If the third timing source is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-82.

Step 4 If the third timing source is an incoming port on the ONS 15327, complete the "Clear the LOS (OC-N) Alarm" procedure on page 2-85.

Step 5 If the third timing source uses the internal ONS 15327 timing, complete the "Reset the Active XTC Card in CTC" procedure on page 2-129.

Verify that the active card you reset is now standby. The ACT/STBY LED of this card should be amber, and the newly active XTC card LED should be green.

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 XTC" procedure on page 3-3. If the TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-130.

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

2.6.182 SYSBOOT

- Major (MJ), Service Affecting (SA)

The System Reboot (SYSBOOT) alarm indicates that new software is booting on the XTC card. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 10 minutes if the same version of software is present on both cards, or up to 30 minutes if the software is being updated from one XTC to the other.

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.

2.6.183 TIM-P

- Critical (CR), Service Affecting (SA) for STSTERM
- Minor (MN), Non-Service Affecting (NSA) for STSMON

The Trace Identifier Mismatch (TIM) Path alarm occurs when the expected path trace string does not match the received path trace string. Path Trace Mode must be set to manual or Auto for the TIM-P alarm to occur.

In manual mode at the Path Trace window, the user types the expected string into the Current Expected String field for the receiving port. The string must match the string typed into the Transmit String field for the sending port. If these fields do not match, the login node raises the TIM-P alarm. In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Complete the following procedure to clear either instance.

TIM-P also occurs on a port that has previously been operating without alarms if someone switches or removes the DS-3 cables or optical fibers that connect the ports. TIM-P is usually accompanied by other alarms, such as an LOS (OC-N) alarm (see page 2-84), an UNEQ-P alarm (see page 2-122), or a PLM-P alarm (see page 2-95). If these alarms accompany TIM-P, reattach or replace the original cables/fibers to clear the alarms.

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** check 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).

2.6.184 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 G1000-2 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 an AIS-P condition (see page 2-17), an LOP-P alarm (see page 2-80), a PDI-P alarm (see page 2-93), or an UNEQ-P alarm (see page 2-122) exist on the SONET path used by the Ethernet port, the affected port causes a TPTFAIL alarm. Also, if the far-end G1000-2 Ethernet port is administratively disabled or it is reporting a CARLOSS (G Series) alarm (see page 2-34), the C2 byte in the SONET path overhead indicates a PDI-P alarm (see page 2-93) which in turn causes a TPTFAIL to be reported against the near-end port.

When a TPTFAIL alarm occurs, the near-end port is automatically disabled (transmit laser turned off). In turn the laser shutoff can also cause the external Ethernet device attached at the near end to detect a link down and turn off its transmitter. This also causes a CARLOSS condition to occur on the reporting port. In all cases the source problem is either in the SONET path being used by the G1000-2 port or the far- end G1000-2 port to which it is mapped.

Clear the TPTFAIL (G-Series) Alarm

Step 1 An occurrence of TPTFAIL on a G1000-2 port indicates either a problem with the SONET path that the port is using or with the far-end G1000-2 port that is mapped to the port. Clear any alarms being reported by the OC-N card on the G1000-2 circuit.

Step 2 If no alarms are reported by the OC-N card, or if a PDI-P alarm (see page 2-93) is reported, the problem might be on the far-end G1000-2 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).

2.6.185 TRMT

- Major (MJ), Service Affecting (SA)

A Missing Transmitter (TRMT) alarm occurs when there is a transmit failure on the XTC-14 card because of an internal hardware failure. The card must be replaced.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the TRMT Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-130 for the reporting XTC-14 card.

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

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).

2.6.186 TRMT-MISS

- Major (MJ), Service Affecting (SA)

A Facility Termination Equipment Transmitter Missing (TRMT-MISS) alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its connector. Incorrect impedance is detected when a transmit cable is missing on the XTC-14 does not match the inserted card; for example, an SMB connector or a BNC connector connects to an XTC-14 card instead of an XTC-28-3 card.

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.**

Note DS-1s are four-wire circuits and need a positive and negative connection for both transmit and receive.

Clear the TRMT-MISS Alarm

Step 1 Verify that the device attached to the XTC-14 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).

2.6.187 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.

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 Deleting a circuit affects traffic.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

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 condition (see page 2-17) is reported on the terminating cards. These alarms clear when the circuit carries a signal.

Clear the UNEQ-P Alarm

Step 1 In node view, click **View > Go to Network View**.

Step 2 Right-click the alarm to display the Select Affected Circuits 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). The node view 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 2-128.
- **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 or not whether there are incomplete circuits:

- **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 2-128.

Step 10 Recreate the circuit with the correct circuit size. Refer to the *Cisco ONS 15327 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 15327 Procedure Guide*.

Step 13 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-130 for the OC-N/DS-N cards.

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).

2.6.188 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 **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 15327. Plug the wristband cable into the ESD jack located between the top high-speed and XTC slots.

Clear the UNEQ-V Alarm

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-123.

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).

2.6.189 WKSWPR

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

The Working Switched To Protection (WKSWPR) condition occurs when a line experiences an LOS (OC-N) alarm (see page 2-84), an SF condition (see page 2-106), or an SD condition (see page 2-104).

Clear the WKSWPR Condition

Step 1 Complete the "Clear the LOF (OC-N) Alarm" 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 to report a service-affecting problem (1-800-553-2447).

2.6.190 WTR

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

The Wait To Restore (WTR) condition occurs when a WKSWPR condition (see page 2-124) 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.

2.7 XTC Line Alarms

The XTC-28-3 card provides three choices of line types: ESF, D4, or Unframed. The choice of framing format determines the line alarms that the XTC-28-3 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 XTC-14 card reports the same STS alarms as the standard XTC-28-3 card does.

Table 2-8 DS3-12E Line Alarms

Alarm	UNFRAMED	D4	ESF
LOS	Yes	Yes	Yes
AIS	Yes	Yes	Yes
LOF	No	Yes	Yes
IDLE	No	Yes	Yes
RAI	No	Yes	Yes
Terminal Lpbk	Yes	Yes	Yes
Facility Lpbk	Yes	Yes	Yes
FE Lpbk	No	No	Yes
FE Common Equipment Failure	No	No	Yes
FE Equipment Failure-SA	No	No	Yes
FE LOS	No	No	Yes
FE LOF	No	No	Yes
FE AIS	No	No	Yes
FE IDLE	No	No	Yes
FE Equipment Failure-NSA	No	No	Yes

2.8 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 15327 Procedure Guide*.

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 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.

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 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.

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 node view, click **View > Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Highlight the ring and click **Edit**.

Step 5 In the BLSR window, right-click the node on the ring map.

Step 6 Select **Set Node ID** from the shortcut menu.

Step 7 Enter the new ID in the field.

Step 8 Click **Apply**.

Verify Node Visibility for Other Nodes

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 At 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**.

Verify or Create Node DCC Terminations

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 At the node view, click the **Provisioning > SONET DCC** tabs.

Step 3 View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to Step 4.

Step 4 If necessary, create a DCC termination:

a. Click **Create**.

b. In the Create SDCC Terminations dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the **Shift** key.

c. In the Port State area, click the **Set to IS** radio button.

d. Verify that the Disable OSPF on Link check box is unchecked.

e. Click **OK**.

Lock Out a BLSR Span

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click the **Maintenance > BLSR** tabs.

Step 3 Click the BLSR row table cell under the West Switch column to reveal the drop-down menu.

Step 4 Choose **LOCKOUT SPAN** and click **Apply**.

Step 5 Click **OK** on the BLSR Operations dialog box.

Clear a BLSR Span Lock Out

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click the **Maintenance > BLSR** tabs.

Step 3 Click the BLSR row table cell under the West Switch column to reveal the drop-down menu.

Step 4 Choose **CLEAR** and click **Apply**.

Step 5 Click **OK** on the BLSR Operations dialog box.

Clear a Path Protection Lock Out

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click **View > Go to Network View**.

Step 3 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 drop-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 UPSR circuits is CLEAR.

Switch Protection Group Traffic with an External Switching Command

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 Display the node view.

Step 3 In node view, click the **Maintenance > Protection** tabs.

Step 4 Double-click the protection group that contains the reporting card.

Step 5 Click the working/active card of the selected groups.

Step 6 Click **FORCE** and **Yes** in the Confirmation dialog box.

Clear an External Switching Command

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click 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.

Delete a Circuit

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click 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.

Clear a Loopback

Step 1 Log into a node on the network. If you are already logged in, go to 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 if any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down menu and select **None**.

Step 6 In the State column, determine whether any port row shows a state other than INS.

Step 7 If a row shows a state other than INS, click in the column cell to display the drop-down menu and select **INS**.

Step 8 Click **Apply**.

Reset the Active XTC Card in CTC

Caution Resetting the active XTC card can be service-affecting.

Note Before you reset the XTC, 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, go to Step 2.

Step 2 Identify the active XTC.

If you are looking at the physical ONS 15327, the ACT/STBY LED of the active XTC is green. The ACT/STBLY LED of the standby XTC is amber.

Step 3 Right-click the active XTC.

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. The reboot takes up to ten minutes.

Step 6 Verify that the reset is complete and error-free:

Double-click the node and ensure that the reset XTC is in standby mode and that the other XTC is active.

- If you are looking at the physical ONS 15327, the ACT/STBY LED of the active XTC is green. The ACT/STBLY LED of the standby XTC is amber.
- No new alarms appear in the **Alarms** window in CTC.
- If you are looking at the physical ONS 15327, the active XTC ACT/STBY LED is green, and the LED of the standby XTC is amber.

Reset a Traffic Card in CTC

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, position the cursor over the high-speed slot 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.

Verify BER Threshold Level

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, double-click the card reporting the alarm to display the card view.

Step 3 Click the **Provisioning > Line** tabs.

Step 4 Under the **SD BER** (or **SF BER**) column on the Provisioning window, verify that the cell entry is consistent with the originally provisioned threshold. The default setting is 1E–7.

Step 5 If the entry is consistent with what the system was originally provisioned for, go back to your original procedure.

Step 6 If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the original entry.

Step 7 Click **Apply**.

Physically Replace a Card

Step 1 Open the card ejectors.

Step 2 Slide the card out of the slot.

Step 3 Open the ejectors on the replacement card.

Step 4 Slide the replacement card into the slot along the guide rails.

Step 5 Close the ejectors.

Remove and Reinsert (Reseat) a Card

Caution Do not perform this action on the XTC card without the supervision and direction of the Cisco Technical Assistance Center (TAC). The Cisco TAC can be reached at (1-800-553-2447).

Step 1 Open the card ejectors.

Step 2 Slide the card halfway out of the slot along the guide rails.

Step 3 Slide the card all the way back into the slot along the guide rails.

Step 4 Close the ejectors.

Remove and Reinsert Fan-Tray Assembly

Step 1 Use the retractable handles embedded in the front of the fan-tray assembly to pull it forward several inches.

Step 2 Push the fan-tray assembly firmly back into the ONS 15327.

Step 3 Close the retractable handles.